PCT/JP2004/002928

05.3.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

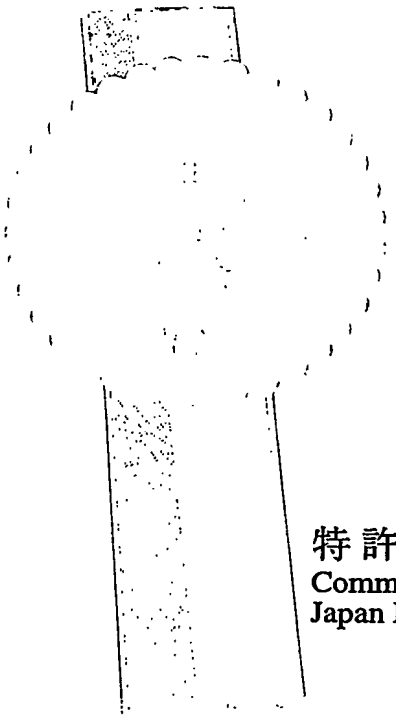
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月　３日

出願番号
Application Number: 特願２００３－１００８６６

[ST. 10/C]: [ＪＰ２００３－１００８６６]

出願人
Applicant(s): 松下電器産業株式会社



２００４年　４月　９日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０２９２８３

【書類名】　特許願
【整理番号】　2054051008
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/032
　　G07C
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　▲浜▼井　信二
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
　【電話番号】　06-4806-7530
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置、証明書発行装置及び通信システム

【特許請求の範囲】

【請求項１】　サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信装置であって、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得手段と、

取得された失効番号を記憶する失効番号記憶手段と、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出し手段と、

読み出された識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断手段と、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御手段と

を備えることを特徴とする通信装置。

【請求項２】　前記有効性判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記サーバ証明書が有効であると判断する

ことを特徴とする請求項１記載の通信装置。

【請求項３】　前記通信装置は、さらに、前記失効番号の有効性を判断する失効番号判断手段を備え、

前記証明書判断手段は、前記失効番号判断手段によって前記失効番号が有効であると判断された場合に、前記失効番号を用いて、前記サーバ証明書の有効性を判断する

ことを特徴とする請求項１記載の通信装置。

【請求項４】　前記失効番号判断手段は、前記リポジトリ装置の正当性を示すリポジトリ証明書の識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号の有効性を判断する

ことを特徴とする請求項３記載の通信装置。

【請求項５】　前記失効番号判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記リポジトリ装置が有効であると判断する

ことを特徴とする請求項４記載の通信装置。

【請求項６】　前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号取得手段によって取得された失効番号の有効性を判断する

ことを特徴とする請求項３記載の通信装置。

【請求項７】　前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号が前記失効番号記憶手段に記憶されている失効番号と同じか大きい場合に、前記失効番号が有効であると判断する

ことを特徴とする請求項６記載の通信装置。

【請求項８】　サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置であって、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶する失効番号記憶手段と、

新たなサーバ証明書を発行する発行手段とを備え、

前記発行手段は、前記失効番号記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行する

ことを特徴とする証明書発行装置。

【請求項９】　前記証明書発行装置は、さらに、失効させるサーバ証明書の識別番号の通知を取得すると、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備える

ことを特徴とする請求項８記載の証明書発行装置。

【請求項１０】　前記証明書発行装置は、さらに、サーバ証明書の有効期限が近づいたサーバ証明書の識別番号を特定し、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備える

ことを特徴とする請求項８記載の証明書発行装置。

【請求項１１】　前記発行手段は、前記失効番号更新手段によって失効番号が更新された場合に、更新後の失効番号よりも小さな値の識別番号をもつサーバ証明書に対応するサーバ装置に対して、新たなサーバ証明書を発行する

ことを特徴とする請求項９又は１０記載の証明書発行装置。

【請求項１２】　サーバ装置と、サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置と、前記サーバ証明書に基づいて前記サーバ装置と通信する通信装置とから構成される通信システムであって、

前記証明書発行装置は、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶する失効番号記憶手段と、

新たなサーバ証明書を発行する発行手段とを備え、

前記発行手段は、前記失効番号記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行し、

前記通信装置は、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得手段と、

取得された失効番号を記憶する失効番号記憶手段と、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出し手段と、

読み出された識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断手段と、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御手段と備える

ことを特徴とする通信システム。

【請求項１３】　サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信方法であって、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得ステップと、

取得された失効番号を記憶手段に格納する失効番号格納ステップと、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出しステップと、

読み出された識別番号と前記記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断ステップと、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御ステップと

を含むことを特徴とする通信方法。

【請求項１４】　サーバ装置の正当性を示すサーバ証明書を発行する証明書発行方法であって、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶手段に格納する失効番号記憶ステップと、

新たなサーバ証明書を発行する発行ステップとを含み、

前記発行ステップでは、前記記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行する

ことを特徴とする証明書発行方法。

【請求項１５】　サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信装置のためのプログラムであって、

前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得ステップと、

取得された失効番号を記憶手段に格納する失効番号格納ステップと、

前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出しステップと、

読み出された識別番号と前記記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断ステップと、

前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御ステップと

をコンピュータに実行させることを特徴とするプログラム。

【請求項１６】　サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置のためのプログラムであって、

サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶手段に格納する失効番号記憶ステップと、

新たなサーバ証明書を発行する発行ステップとをコンピュータに実行させ、

前記発行ステップでは、前記記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行する

ことを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信装置、証明書発行装置及び通信システム等に関し、通信時においてサーバ証明書を用いてサーバ認証を行う通信装置、証明書発行装置及び通信システム等に関する。

【０００２】

【従来の技術】

インターネットにおけるサーバ・クライアント間の通信時における盗聴、サーバなりすましに対抗する技術としてＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）が特許文献１に、ＳＳＬを改良したＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ）が特許文献２に記載されている（以下総称してＳＳＬと呼ぶ）。

【０００３】

図１５は、ＳＳＬ通信時における通信システムのシステム構成を示すブロック図である。

【０００４】

通信システムは、認証局（ＣＡ）が運営するサーバ証明書作成装置１０００及びリポジトリ２０００と、アプリケーション提供者が使用する複数のアプリケーションサーバ３０００ａ～３０００ｋと、ユーザが使用する複数の端末４０００

ａ～４０００ｎとから構成される。リポジトリ２０００、各アプリケーションサーバ３０００ａ～３０００ｋ及び各端末４０００ａ～４０００ｎは、インターネット５０００に接続されている。

【０００５】

サーバ証明書作成装置１０００は、各端末４０００ａ～４０００ｎに対してＣＡ証明書６０００を発行したり、アプリケーションサーバ３０００ａ～３０００ｋに対してサーバ証明書７０００を発行したり、リポジトリ２０００に対してサーバ証明書無効化リスト（以下、「ＣＲＬ」とも記す。）８０００を配信したりするコンピュータ装置である。

【０００６】

リポジトリ２０００は、配信を要求した端末４０００ａ～４０００ｎに対してＣＲＬ８０００を配信するコンピュータ装置であり、サーバ証明書作成装置１０００から配信されてきたＣＲＬ８０００を蓄積するＣＲＬ蓄積部２１００と、各端末４０００ａ～４０００ｎからの配信要求を受け付けて、ＣＲＬ蓄積部２１００に蓄積されているＣＲＬ８０００を配信を要求した端末４０００ａ～４０００ｎに対して送信する通信部２２００とを備える。

【０００７】

各アプリケーションサーバ３０００ａ～３０００ｋは、ＳＳＬ通信時に通信を要求した端末４０００ａ～４０００ｎに対してサーバ証明書７０００を配信するコンピュータ装置であり、サーバ部３１００と、サーバ証明書蓄積部３２００と、通信部３３００とを備える。

【０００８】

各端末４０００ａ～４０００ｎは、クライアント部４１００と、ＣＡ証明書蓄積部４２１０及びＣＲＬ蓄積部４２２０を有するサーバ証明書検証部４２００と、時計４３００と、通信部４４００とを備える。

【０００９】

端末４０００ａ～４０００ｎがアプリケーションサーバ３０００ａ～３０００ｋと通信を行うまえにあらかじめ認証局はサーバ証明書作成装置１０００でサーバ証明書を発行し、各アプリケーションサーバ３０００ａ～３０００ｋにサーバ

証明書７０００を配布する。アプリケーションサーバ３０００ａ～３０００ｋは配布されたサーバ証明書７０００をサーバ証明書蓄積部３２００に蓄積する。

【００１０】

また、サーバ証明書７０００を署名するＣＡの秘密鍵のペアとなるＣＡの公開鍵を含むＣＡ証明書６０００を端末４０００ａ～４０００ｎに配布し、端末４０００ａ～４０００ｎはＣＡ証明書６０００をＣＡ証明書蓄積部４２１０に蓄積する。

【００１１】

一方、認証局は、サーバ証明書７０００の無効を調査し、無効と判断すればサーバ証明書作成装置１０００でそのサーバ証明書７０００のシリアルをリストに加えた新たなＣＲＬ８０００を作成し、リポジトリ２０００に配布する。

【００１２】

リポジトリ２０００は、ＣＲＬ蓄積部２１００にＣＲＬ８０００を蓄積する。端末４０００ａ～４０００ｎは、定期的にリポジトリ２０００の通信部２２００にＣＲＬ８０００の配信を要求する。

【００１３】

端末４０００ａ～４０００ｎからの要求に応じてＣＲＬ８０００を端末４０００ａ～４０００ｎに配布する。リポジトリ２０００はＣＲＬ蓄積部２１００からＣＲＬ８０００を取り出し、ＣＲＬ８０００を通信部２２００から端末４０００ａ～４０００ｎの通信部４４００に送信する。端末４０００ａ～４０００ｎは受信したＣＲＬ８０００をＣＡ証明書蓄積部４２１０に保管する。

【００１４】

図１６は、図１５に示されるサーバ証明書７０００の最小限の構成例を示す図である。なお、ＳＳＬではサーバ証明書としてｘ５０９形式が使用される。

【００１５】

サーバ証明書７０００は、バージョン７００１と、シリアル７００２と、署名アルゴリズム７００３と、発行者７００４と、有効期間７００５と、名前７００６と、公開鍵７００７と、署名７００８とから構成される。

【００１６】

バージョン７００１は、ｘ５０９のバージョンを示す。シリアル７００２は、発行者によってサーバ証明書に付与されるユニークな番号である。署名アルゴリズム７００３は、発行者が署名する際のアルゴリズムを示す。発行者７００４は、このサーバ証明書を発行した認証局の名前である。有効期間７００５は、サーバ証明書が有効な期間を示す。名前７００６は、サーバ証明書の発行先の名前である。公開鍵７００７は、サーバの公開鍵である。署名７００８は、このサーバ証明書の署名を除く部分に対して認証局が認証局のＣＡ秘密鍵を用いて署名した署名である。

【００１７】

図１７は、図１５に示されるＣＲＬ８０００の最小限の構成を示す図である。

ＣＲＬ８０００は、バージョン８００１と、署名アルゴリズム８００２と、発行者８００３と、更新時間８００４と、次回更新時間８００５と、失効証明書８００６と、署名アルゴリズム８００７と、署名８００８とから構成される。

【００１８】

バージョン８００１は、失効証明書リストのバージョンである。署名アルゴリズム８００２は、発行者が署名した際のアルゴリズムを示す。発行者８００３は、ＣＲＬ８０００の発行者である認証局の名前である。更新時間８００４は、この失効証明書リストの発行された時間であり、次回更新時間８００５は、次に更新する予定時間である。失効証明書８００６は、失効したサーバ証明書のシリアル８００６ａとその失効時間８００６ｂのリストである。認証局が発行者の名前で発行したサーバ証明書のうち、認証局が失効したと判断したサーバ証明書のシリアルがシリアル８００６ａにその失効した時間８００６ｂとともに記載される。署名アルゴリズム８００７は、発行者が署名した際のアルゴリズムを示す。署名８００８は、ＣＲＬ８０００の署名を除く部分に対して認証局がＣＡ秘密鍵を用いて署名した署名である。

【００１９】

次いで、端末４０００ａ～４０００ｎ及びアプリケーションサーバ３０００ａ～３０００ｋ間で暗号化せずに通信を行う場合について説明する。

【００２０】

図１８は、暗号化せずに通信を行う場合のシーケンス図である。なおここでは、端末４０００ａとアプリケーションサーバ３０００ａとの間で行われた場合をその代表例として説明する。

【００２１】

端末４０００ａのクライアント部４１００は、アプリケーションサーバ３０００ａに対してリクエスト１を送るように通信部４４００に指示をする（Ｓ８０１）。通信部４４００は、アプリケーションサーバ３０００ａの通信部３３００に対してリクエスト１を送信する（Ｓ８０２）。

【００２２】

アプリケーションサーバ３０００ａの通信部３３００は、受信したリクエスト１をサーバ部３１００に出力する（Ｓ８０３）。サーバ部３１００はリクエスト１を処理してレスポンス１を生成し、端末４０００ａに送るよう通信部３３００に指示する（Ｓ８０４）。通信部３３００は、端末４０００ａの通信部４４００にレスポンス１を送信する（Ｓ８０５）。

【００２３】

端末４０００ａの通信部４４００は、レスポンス１をクライアント部４１００に出力する（Ｓ８０６）。

【００２４】

このようなシーケンスでリクエスト１、レスポンス１が暗号化されずに通信が行われる。

【００２５】

次に端末４０００ａ～４０００ｎ及びアプリケーションサーバ３０００ａ～３０００ｋ間で暗号化して通信を行う場合について説明する。

【００２６】

図１９は、暗号化して通信を行う場合のシーケンス図である。なおここでは、端末４０００ａとアプリケーションサーバ３０００ａとの間で行われた場合をその代表例として説明する。

【００２７】

端末４０００ａのクライアント部４１００は、リクエスト２を暗号化してアプ

リケーションサーバ３０００ａに送るよう通信部４４００に指示を行う（Ｓ９００）。通信部４４００は、共有鍵の種のひとつとなるクライアント乱数と通信部４４００が処理できる暗号の種類を含んだＣｌｉｅｎｔＨｅｌｌｏパケットをアプリケーションサーバ３０００ａの通信部３３００に送信し、ＳＳＬのハンドシェークを開始する（Ｓ９０１）。

【００２８】

アプリケーションサーバ３０００ａの通信部３３００は、ＣｌｉｅｎｔＨｅｌｌｏパケットから暗号の種類を決定し、共有鍵の種の一つとなるサーバ乱数とこの通信を一意に特定するセッションＩＤを生成し、決定した暗号の種類とサーバ乱数とセッションＩＤをＳｅｒｖｅｒＨｅｌｌｏパケットで送り（Ｓ９０２）、サーバ証明書蓄積部３２００からサーバ証明書を取り出し（Ｓ９０３）、サーバ証明書７０００をＣｅｒｔｉｆｉｃａｔｅパケットとして端末４０００ａの通信部４４００に送信し（Ｓ９０４）、さらにＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅパケットを通信部４４００に送る（Ｓ９０７）。

【００２９】

端末４０００ａの通信部４４００は、Ｃｅｒｔｉｆｉｃａｔｅパケットからサーバ証明書７０００を取り出し、サーバ証明書検証部４２００に送る（Ｓ９０５）。サーバ証明書検証部４２００は、サーバ証明書が不正でないか検証し、検証結果を通信部４４００に通知する（Ｓ９０６）。サーバ証明書が不正であれば、通信部４４００は、アラートパケットをアプリケーションサーバ３０００ａの通信部３３００に送信して通信を切断し、クライアント部４１００にエラーを返す。これに対して、サーバ証明書が不正でない場合には、通信部４４００は、暗号化の共有鍵を計算するためのプリマスターシークレットを作成して、サーバ証明書７０００に含まれるサーバ公開鍵で暗号化し、ＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅパケットの到着後に暗号化されたプリマスターシークレットを含むＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅパケットをアプリケーションサーバ３０００ａの通信部３３００に送信し（Ｓ９０８）、さらにＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃパケットを通信部３３００に送信する（Ｓ９０９）。ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃパケットは、暗号化の開始を示すパケットである。通信部４４００は、ク

ライアント乱数とサーバ乱数とプリマスターシークレットから暗号化に使用する共通鍵Ｃを作成し、ハンドシェークの終了を示すＦｉｎｉｓｈｅｄパケットを作成した共通鍵Ｃで暗号化してアプリケーションサーバ３０００ａの通信部３３００に送信する（Ｓ９１０）。

【００３０】

アプリケーションサーバ３０００ａの通信部３３００は、ＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅから暗号化されたプリマスターシークレットを取り出し、サーバ秘密鍵を用いてプリマスターシークレットに復号し、サーバ乱数、クライアント乱数とともに暗号化に使用する共通鍵Ｄを作成する。ＳＳＬのハンドシェークが正常に行われた場合、通信部３３００の持つ共通鍵Ｃと通信部４４００の持つ共通鍵Ｄは同一となる。通信部３３００は、受信したＦｉｎｉｓｈｅｄパケットを共通鍵Ｄで復号し、正常に復号できればＦｉｎｉｓｈパケットを暗号化して端末４０００ａの通信部４４００に送信する（Ｓ９１１）。このＦｉｎｉｓｈｅｄ以降の通信は、すべて暗号化して行われる。

【００３１】

端末４０００ａの通信部４４００は、受信したＦｉｎｉｓｈｅｄパケットを復号し、正常に復号できれば、リクエスト２を暗号化してアプリケーションサーバ３０００ａの通信部３３００に送付する（Ｓ９１２）。

【００３２】

アプリケーションサーバ３０００ａの通信部３３００は、リクエスト２を復号し、サーバ部３１００に送る（Ｓ９１３）。サーバ部３１００は、リクエスト２を処理してレスポンス２を生成し、端末４０００ａ～４０００ｎａに送るよう通信部３３００に指示する（Ｓ９１４）。通信部３３００は、端末４０００ａの通信部４４００にレスポンス２を暗号化して送信する（Ｓ９１５）。

【００３３】

端末４０００ａの通信部４４００は、レスポンス２を復号してクライアント部４１００に出力する（Ｓ９１６）。

以上のように暗号化を行い通信する。

【００３４】

次いで、サーバ証明書検証部４２００が行う検証について説明する。

図２０は、サーバ証明書検証部４２００が行うサーバ証明書７０００の検証動作を示すフローチャートである。

【００３５】

サーバ証明書検証部４２００は、受信したサーバ証明書７０００から有効期間７００５を取り出し、また時計４３００から現在時刻を取得する（Ｓ９０５１）。次いでサーバ証明書検証部４２００は、有効期間７００５の始期及び終期と現在時間をそれぞれ比較し、現在時間がサーバ証明書の有効期間７００５でなければ期限外のエラーコードを通信部４４００に通知して検証を終了する（Ｓ９０５７）。

【００３６】

これに対して現在時間がサーバ証明書の有効期間７００５内であれば、サーバ証明書７０００の発行者７００４を取り出し、さらに保管しているＣＡ証明書蓄積部４２１０から、発行者７００４のＣＡ証明書６０００を検索する。発行者のＣＡ証明書６０００があればそのＣＡ証明書６０００からＣＡの公開鍵を取り出し、ＣＡの公開鍵を用いてサーバ証明書７０００の署名７００８のチェックを行う。署名７００８が不正であれば、署名の検証エラーのエラーコードを通信部４４００に通知して検証を終了する（Ｓ９０５７）。

【００３７】

署名（１２０８）が正しければ、サーバ証明書検証部４２００は、サーバ証明書７０００からシリアル７００２を取り出す。そしてＣＲＬ蓄積部４２２０からＣＲＬ８０００を取り出し、取り出したシリアルがＣＲＬ８０００に含まれているかどうかをチェックする。もし含まれていればそのサーバ証明書は失効していると判断し、失効のエラーコードを通信部４４００に通知して検証を終了する（Ｓ９０５７）。もし含まれていないならばそのサーバ証明書は正しいと判断して通信部４４００に正常終了を通知する。

【００３８】

以上のように端末４０００ａ～４０００ｎはアプリケーションサーバ３０００と通信する際にＳＳＬを用いた暗号化通信を行い、盗聴とサーバのなりすましを

防止する。

【００３９】

【特許文献１】

Ｕ．Ｓ．Ｐａｔｅｎｔ　５６５７３９０

【００４０】

【特許文献２】

ＲＦＣ２２４６（ＩＥＴＦ）

【００４１】

【発明が解決しようとする課題】

しかしながら、従来の方法では次の点に課題がある。

【００４２】

まず、従来の通信システムではＣＲＬの大きさが固定でなく、サーバ証明書の失効が増えるとともにＣＲＬのサイズが非常に大きくなる（数十～数百ｋバイト）。このことから端末においてＣＲＬを蓄積する容量として大きなものを用意しなければならないという課題がある。また、ＣＲＬが大きくなった場合、サーバ証明書の検証時にサーバ証明書のシリアルがＣＲＬのリストに含まれているかどうか検索する時間が大きくなるという課題がある。また、ＣＲＬが大きくなった場合、端末がリポジトリからＣＲＬを取得する際の通信路の容量及びリポジトリの処理能力に大きなものが必要となるという課題がある。

【００４３】

さらにサーバ証明書の有効期間検証の際に現在時間と比較するために正確な時計が必要であるという課題がある。

【００４４】

すなわち、サーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信するため、従来のシステムでは端末（通信装置）などに容量の大きなメモリや、精度の高い時計、通信インターフェースなど十分なリソースが必要であった。

【００４５】

本発明は、上述の技術的課題を解決し、簡単なリソースでサーバ装置の正当性

を示すサーバ証明書に基づいて当該サーバ装置と通信することができる通信装置、証明書発行装置及び通信システム等を提供することを目的とする。

【００４６】

【課題を解決するための手段】

上記目的を達成するために、本発明に係る通信装置は、サーバ装置の正当性を示すサーバ証明書に基づいて前記サーバ装置と通信する通信装置であって、前記サーバ証明書の有効性を判断する基準となる情報である失効番号を保持するリポジトリ装置から、前記失効番号を取得する失効番号取得手段と、取得された失効番号を記憶する失効番号記憶手段と、前記サーバ証明書を識別する識別番号を前記サーバ証明書から読み出す識別番号読み出し手段と、読み出された識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記サーバ証明書の有効性を判断する証明書判断手段と、前記サーバ証明書が有効であると判断された場合に、前記サーバ装置との通信を確立し、前記サーバ証明書が有効でないと判断された場合に、前記サーバ装置との通信を確立しない通信制御手段とを備えることを特徴とする。

【００４７】

具体的には、前記有効性判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記サーバ証明書が有効であると判断することを特徴としてもよい。

【００４８】

これにより、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断したり、従来のようにリポジトリからサイズの大きなＣＲＬを取得して、たくさんのリストを記憶し、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検索したりする必要がなくなり、通信装置は、リポジトリから失効番号を１つだけ取得し、これを記憶している１つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

【００４９】

また、前記通信装置は、さらに、前記失効番号の有効性を判断する失効番号判断手段を備え、前記証明書判断手段は、前記失効番号判断手段によって前記失効番号が有効であると判断された場合に、前記失効番号を用いて、前記サーバ証明書の有効性を判断することを特徴としてもよい。具体的には、前記失効番号判断手段は、前記リポジトリ装置の正当性を示すリポジトリ証明書の識別番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号の有効性を判断することを特徴とすることができ、また、前記失効番号判断手段は、前記識別番号が前記失効番号と同じか大きい場合に、前記リポジトリ装置が有効であると判断することを特徴とすることができる。

【００５０】

これにより、通信装置は、サーバ装置との通信と同じ手順でリポジトリ証明書を取得し、リポジトリ証明書を用いてリポジトリを認証したり、リポジトリが正当である場合に失効番号を暗号通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

【００５１】

また、前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号と前記失効番号記憶手段に記憶されている失効番号とを比較することによって前記失効番号取得手段によって取得された失効番号の有効性を判断することを特徴とすることができ、具体的には、前記失効番号判断手段は、前記失効番号取得手段によって取得された失効番号が前記失効番号記憶手段に記憶されている失効番号と同じか大きい場合に、前記失効番号が有効であると判断することを特徴とする。

【００５２】

これにより、通信装置は、リポジトリが正当である場合に失効番号を暗号なしの通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

【００５３】

また、サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置であって、サーバ証明書の有効性を判断する基準となる情報である失効番号を記憶する失効番号記憶手段と、新たなサーバ証明書を発行する発行手段とを備え、前記発行手段は、前記失効番号記憶手段に記憶されている失効番号と同じか大きい値を示す識別番号を含ませて、前記サーバ証明書を発行することを特徴とする。

【００５４】

具体的には、前記証明書発行装置は、さらに、失効させるサーバ証明書の識別番号の通知を取得すると、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備えることを特徴とすることができる。

【００５５】

これにより、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断させたり、従来のようにリポジトリからサイズの大きなＣＲＬを取得させたりして、たくさんのリストを記憶させたりし、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検索させたりする必要がなくなり、通信装置は、リポジトリから失効番号を１つだけ取得し、これを記憶している１つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

【００５６】

また、前記証明書発行装置は、さらに、サーバ証明書の有効期限が近づいたサーバ証明書の識別番号を特定し、前記失効番号記憶手段に記憶されている失効番号を前記識別番号よりも大きい番号に更新する失効番号更新手段を備えることを特徴とする。

【００５７】

これにより、有効期間が近づいたサーバー証明書を失効させることができる。

【００５８】

また、前記発行手段は、前記失効番号更新手段によって失効番号が更新された

場合に、更新後の失効番号よりも小さな値の識別番号をもつサーバ証明書に対応するサーバ装置に対して、新たなサーバ証明書を発行することを特徴とする。

【００５９】

これによりサーバ装置は、新たなサーバ証明書を用いて認証を受けることができる。

【００６０】

なお、本発明は、このような通信装置、証明書発行装置として実現することができるだけでなく、このサーバ装置と、サーバ装置の正当性を示すサーバ証明書を発行する証明書発行装置と、前記サーバ証明書に基づいて前記サーバ装置と通信する通信装置とから構成される通信システムとして実現したり、このような通信装置、証明書発行装置が備える特徴的な手段をステップとする通信方法、証明書発行方法として実現したり、それらのステップをコンピュータに実行させるプログラムとして実現したりすることもできる。そして、そのようなプログラムは、ＣＤ－ＲＯＭ等の記録媒体やインターネット等の伝送媒体を介して配信することができるのは言うまでもない。

【００６１】

【発明の実施の形態】

（実施の形態１）

以下、本発明の実施の形態１に係る通信システムついて説明する。

【００６２】

図１は、本発明の実施の形態１に係る通信システム１の全体構成を示すブロック図である。

【００６３】

この通信システム１は、公開鍵暗号方式を使って安全な通信を行うためのインフラＰＫＩ（Public Key Infrastructure）を提供するために、ＣＡ証明書６０、サーバ証明書７５及び失効情報９０を基本のツールとして、アプリケーションサーバを認証するシステムであり、認証局（以下、「ＣＡ」とも記す。）が使用するサーバ証明書作成装置１０及びリポジトリ２０と、映像コンテンツなどのアプリケーション提供者が使用する複数のアプリケーションサーバ３０ａ～３０ｋ

と、ユーザが使用する複数の端末４０ａ～４０ｎと、リポジトリ２０、アプリケーションサーバ３０ａ～３０ｋ及び端末４０ａ～４０ｎを接続するインターネット５０とから構成される。なお、各アプリケーションサーバ３０ａ～３０ｋが同じ構成であるのでの同図においてはアプリケーションサーバ３０ａの詳細構成だけが図示されており、また端末４０ａ～４０ｎが同じ構成であるので同図においてはアプリケーションサーバ３０ａの詳細構成だけが図示されている。

【００６４】

サーバ証明書作成装置１０は、ワークステーション等のコンピュータ装置であり、通信システム１における基本のツールを提供する基本的なサーバとして機能する。具体的には、サーバ証明書作成装置１０は、端末４０ａ～４０ｎに対してＣＡ証明書６０を予め発行したり、アプリケーションサーバ３０ａ～３０ｋからの証明書要求（Certificate Signing Request、以下、「ＣＳＲ」とも記す。）７０に応じて、「０」から「１」ずつ単調に増加され、かつこのシステムにおいてユニークなシリアルを含み、かつ各アプリケーションサーバ３０ａ～３０ｋに専用のサーバ証明書７５を発行したり、サーバ証明書７５の有効期限が近づいたような場合においてサーバ証明書７５を失効させるとき、該当するアプリケーションサーバに対して証明書失効（証明書更新要求）を予め通知したり、「０」から必要数単調に増加され、サーバ証明書７５が失効しているか否かを判断するためのシリアル（以下、「失効シリアル」あるいは「失効番号」とも記す。）を含む失効情報９０をリポジトリ２０に送信したりする。

【００６５】

なお、ＣＡ証明書６０は、例えばこの証明書の発行者と、署名アルゴリズムと、この証明書の有効期間（例えば、１０年）と、ＣＡの公開鍵（ＣＡ公開鍵）と、このＣＡ公開鍵とペアのＣＡの秘密鍵（ＣＡ秘密鍵）による署名とが含められて構成されている。また、ＣＳＲ７０は、ＣＳＲを発したサーバの名前と、そのサーバの公開鍵（サーバ公開鍵）とが含められて構成されている。

【００６６】

リポジトリ２０は、ワークステーション等のコンピュータ装置であり、サーバ証明書作成装置１０から通知された最新の失効情報９０を蓄積し、インターネッ

ト５０を介して端末４０ａ～４０ｎから失効情報９０の要求（リクエスト）があると、要求した端末４０ａ～４０ｎに失効情報９０をレスポンスとして暗号なしの通信で配信する。

【００６７】

アプリケーションサーバ３０ａ～３０ｋは、ワークステーション等のコンピュータ装置であり、サーバ証明書作成装置１０から証明書失効通知があった場合など、必要に応じてサーバの名前及びそのサーバの公開鍵を含むＣＳＲ７０をサーバ証明書作成装置１０に対して行い、サーバ証明書作成装置１０が発行した自己専用のサーバ証明書７５を保持する。そして、アプリケーションサーバ３０ａ～３０ｋは、端末４０ａ～４０ｎからアプリケーションのダウンロードなどの要求（リクエスト）があった際にＳＳＬの通信プロトコルに従ってサーバ証明書７５を送信し、認証を受けた後セッション鍵（共有鍵）を用いて暗号通信で要求されたアプリケーションをレスポンスとして配信する。なお、暗号化せずに通信を行う場合は、従来と同様の手順が用いられる。

【００６８】

端末４０ａ～４０ｎは、ネット家電（例えば、ビデオレコーダ）などのコンピュータ装置であり、サーバ証明書作成装置１０が発行したＣＡ証明書６０を予め取得し、これを保持する。また、各端末４０ａ～４０ｎは、リポジトリ２０に対して定期的（例えば１月に１回）の通信部２０２に失効情報９０の配信を要求し、配信されてきた失効情報９０に含まれる最新の失効番号を保持する。そして、端末４０ａ～４０ｎは、アプリケーションをダウンロードする際にＳＳＬの通信プロトコルに従ってアプリケーションサーバ３０ａ～３０ｋから送信されてきたサーバ証明書７５と、予め保持するＣＡ証明書６０と、失効情報９０の失効番号とに基づいてサーバを認証し、サーバ認証後セッション鍵を用いてリクエスト及びレスポンスを暗号通信する。

【００６９】

これによって、リクエスト及びレスポンスの盗聴とを防止する。

【００７０】

図２は、図１に示されるサーバ証明書７５の構成例を示す図である。なお、こ

のサーバ証明書７５においても、従来と同様、サーバ証明書としてｘ５０９形式が使用される。

【００７１】

このサーバ証明書７５は、バージョン７５１と、シリアル７５２と、署名アルゴリズム７５３と、発行者７５４と、有効期間７５５と、サーバの名前７５６と、サーバ公開鍵７５７と、署名７５８との各フィールドから構成される。

【００７２】

バージョン７５１は、ｘ５０９のバージョンを示し、例えば「２」が格納される。シリアル７５２は、発行者によってサーバ証明書に付与されるユニークな番号であり、例えば「０ｘ００１１」（図示例では２バイト）が格納される。署名アルゴリズム７５３は、発行者が署名する際のアルゴリズムを示す。発行者７５４は、このサーバ証明書を発行した認証局の名前であり、例えば「Ｐａｎａｓｉｇｎ」が格納される。有効期間７５５は、サーバ証明書が有効な期間を示し、例えばこのサーバ証明書７５が発行された時刻（有効期間の始期、２００３年、４月１日…）と、１３月後の時刻（有効期間の終期、２００４年、５月１日…）とが格納される。名前７５６は、サーバ証明書の発行先の名前であり、例えば「針ウド映画」が格納される。サーバ公開鍵７５７は、サーバの公開鍵であり、例えば針ウド映画の公開鍵、Ｐｕｂｋ＿１１が格納される。署名７５８は、このサーバ証明書の署名を除く部分の特徴、いわゆる指紋に対する署名であり、例えばサーバの名前針ウド映画とサーバ公開鍵Ｐｕｂｋ＿１１との連結を認証局のＣＡ秘密鍵で暗号化した値が格納される。

【００７３】

このように構成されたサーバ証明書７５をアプリケーションサーバ３０ａ～３０ｋからもらった端末４０ａ～４０ｎは、署名７５８を認証局のＣＡ公開鍵で復号化することによって、サーバ証明書７５が認証局によって正規に発行されたものかを検証したりすることが可能となる。

【００７４】

図３は、図１に示される失効情報９０の構成例を示す図である。

【００７５】

図３に示されるように失効情報９０は、発行者９１と、失効番号９２と、署名９３の各フィールドから構成される。

【００７６】

発行者９１は、失効情報９０の発行者である認証局ＣＡの名称であって、失効情報９０が対象とするサーバ証明書７５の発行者７５４と同一であり、Ｐａｎａｓｉｇｎが格納される。失効番号９２は、発行者が発行しているサーバ証明書７５の内、その時点で有効な最小のシリアルであり、例えば、０ｘ００１１（図示例では２バイト）だけが格納される。署名９３は、このサーバ証明書の署名を除く部分の特徴、発行者９１及び失効番号９２に対する署名であり、例えば発行者９１と失効番号９２との連結をＣＡ秘密鍵で暗号化した値が格納される。

【００７７】

このように構成された失効情報９０をリポジトリ２０からもらった端末４０ａ～４０ｎは、署名９３を認証局のＣＡ公開鍵で復号化することによって、失効情報９０が認証局によって正規に発行されたものかを検証したり、アプリケーションサーバ３０ａ～３０ｋからもらったサーバ証明書７５のシリアルと失効番号９２との大小関係とからそのサーバ証明書７５が失効しているか否かを判断したりすることが可能となる。

【００７８】

次いで、サーバ証明書作成装置１０、リポジトリ２０、アプリケーションサーバ３０ａ～３０ｋ及び端末４０ａ～４０ｎの各構成を順次さらに詳細に説明する。

【００７９】

図１に示されるようにサーバ証明書作成装置１０は、鍵ペア作成部１０１と、ＣＡ証明書作成部１０２と、ＣＡ秘密鍵蓄積部１０３と、時計１０４と、シリアル蓄積部１０５と、ＣＳＲ受信部１０６と、サーバ証明書組立部１０７と、署名部１０８と、サーバ証明書送信部１０９と、サーバ証明書履歴蓄積部１１０と、サーバ証明書期限検索部１１１と、サーバ証明書失効通知部１１２と、失効証明書検索部１１３と、証明書失効通知部１１４と、失効番号蓄積部１１５と、失効情報署名部１１６と、失効情報通知部１１７等とを備える。

【００８０】

鍵ペア作成部１０１は、サーバ証明書７５の署名を行うためのＣＡ秘密鍵と、署名の検証を行うためのＣＡ公開鍵とを作成する。そして鍵ペア作成部１０１は、作成したＣＡ公開鍵及びＣＡ秘密鍵をＣＡ証明書作成部１０２に出力し、ＣＡ秘密鍵をＣＡ秘密鍵蓄積部１０３に出力する。

【００８１】

ＣＡ証明書作成部１０２は、鍵ペア作成部１０１で作成されたＣＡ公開鍵などと、鍵ペア作成部１０１で作成されたＣＡ秘密鍵で署名とでＣＡ証明書６０を作成し、端末４０ａ～４０ｎに送る。

【００８２】

ＣＡ秘密鍵蓄積部１０３は、鍵ペア作成部１０１で作成されたＣＡ秘密鍵を蓄積する。

時計１０４は、現在時刻を正確に計時する。

【００８３】

シリアル蓄積部１０５は、次に発行するサーバ証明書７５に付与されるべきシリアルを蓄積する。具体的には、サーバ証明書作成装置１０でシリアル「４」のサーバ証明書７５まで既に発行している場合には、シリアル蓄積部１０５は、シリアル「５」を蓄積する。なお、シリアル蓄積部１０５が蓄積するシリアルの初期値は「０」である。

【００８４】

ＣＳＲ受信部１０６は、各アプリケーションサーバ３０ａ～３０ｋからＣＳＲ７０を受信すると、受信したＣＳＲ７０をサーバ証明書組立部１０７に出力する。なお、ＣＳＲ７０は、サーバの名前及びサーバ公開鍵を含めて構成される。

【００８５】

サーバ証明書組立部１０７は、サーバ証明書７５に必要な情報を組み立てる。具体的には、サーバ証明書組立部１０７は、シリアル蓄積部１０５から読み出したシリアルをシリアル７５２に設定し、また時計１０４から取得した現在時刻を有効期間７５５の始期に設定し、現在時刻から１３ヶ月後の時刻を有効期間７５５の終期、すなわち有効期限に設定する。そして、サーバ証明書組立部１０７は

、ＣＳＲ７０に含まれる名前及びサーバ公開鍵を名前７５６及びサーバ公開鍵７５７にそれぞれ設定し、予め定められたバージョン、発行者、署名アルゴリズムをバージョン７５１、発行者７５４、署名アルゴリズム７５３にそれぞれ設定し、サーバ証明書７５に必要な情報を署名部１０８に出力する。

【００８６】

そして、サーバ証明書７５に必要な情報を組み立てが終わると、サーバ証明書組立部１０７は、サーバ証明書７５に必要な情報の内、名前７５６、シリアル７５２、有効期間７５５の終期（有効期限）を出力し、サーバ証明書履歴蓄積部１１０のサーバ証明書履歴テーブル１１０ａに蓄積させる。さらに、サーバ証明書組立部１０７は、発行するサーバ証明書７５のシリアルに１加えたもの（例えば、新規発行されるサーバ証明書７５のシリアルが「０ｘ００１０」であれば「０ｘ００１１」）を次に付与すべきシリアルとしてシリアル蓄積部１０５に蓄積させる。

【００８７】

署名部１０８は、ＣＡ秘密鍵蓄積部１０３からＣＡ秘密鍵を取り出し、サーバ証明書組立部１０７から出力されたバージョン７５１、シリアル７５２、署名アルゴリズム７５３、発行者７５４、有効期間７５５、名前７５６、サーバ公開鍵７５７に対して取り出したＣＡ秘密鍵を関与させること署名７５８を作成し、サーバ証明書７５を完成させた後、このサーバ証明書７５をサーバ証明書送信部１０９に出力する。

【００８８】

サーバ証明書送信部１０９は、署名部１０８から出力されたサーバ証明書７５をＣＳＲ７０を発したアプリケーションサーバ３０ａ～３０ｋに送信する。この際、サーバ証明書送信部１０９は、新たなサーバ証明書７５の送信を失効証明書検索部１１３に通知する。

【００８９】

サーバ証明書履歴蓄積部１１０は、サーバ証明書組立部１０７がサーバ証明書７５を組み立てるごとに、そのサーバの名前、サーバ証明書のシリアル、有効期限をサーバ証明書履歴テーブル１１０ａに順次蓄積する。

【００９０】

図４は、サーバ証明書履歴蓄積部１１０が蓄積するサーバ証明書履歴テーブル１１０ａの構成例を示す図である。

【００９１】

図４に示されるようにサーバ証明書履歴テーブル１１０ａは、この通信システム１において現在有効なサーバ証明書７５におけるサーバの名前１１０１、サーバ証明書のシリアル１１０２及び有効期限１１０３をそれぞれ格納するフィールドと、複数のレコードとからなる。

【００９２】

このように構成されたサーバ証明書履歴テーブル１１０ａを用いると、サーバの名前１１０１でサーバ証明書７５を保持するアプリケーションサーバ３０ａ～３０ｋを特定したり、シリアル１１０２で現在有効なサーバ証明書７５のシリアルの最小値（Ｓｅ　ｍｉｎ、図示例では「０ｘ００１１」）やシリアルの最大値（Ｓｅ　ｍａｘ、図示例では「０ｘ０１１０」）を特定したり、有効期限の到来によるサーバ証明書の失効等を管理したりすることができる。

【００９３】

サーバ証明書期限検索部１１１は、定期的にサーバ証明書履歴蓄積部１１０に蓄積されているサーバ証明書履歴テーブル１１０ａの有効期限を参照し、有効期限が１月以内に迫ったサーバ証明書７５を検索する。具体的には、サーバ証明書期限検索部１１１は、時計１０４から現在時刻を読み取り、現在時刻から１ヶ月後までの間に有効期限が切れるサーバ証明書７５を検索する。そしてもし現在時刻から１ヵ月後までの間に有効期限が切れるサーバ証明書７５が存在すれば、その有効期限が迫ったサーバ証明書７５のシリアル（例えば、図４において針ウド映画と大波ゲームの有効期限が１月以内に迫っている場合には、大きな値を有する大波ゲームのシリアル「０ｘ００１２」）を実際に失効させるべきシリアルとして失効証明書検索部１１３に通知する。

【００９４】

サーバ証明書失効通知部１１２は、失効させるサーバ証明書７５のシリアルの入力を受け付けて、そのシリアルを失効証明書検索部１１３に通知する。すなわ

ち、認証局では、アプリケーションサーバのサーバ証明書７５の安全性を常にチェックしており、次の（１）～（３）の場合等に、認証局はサーバ証明書失効通知部１１２から失効させるサーバ証明書７５のシリアル（例えば、図４においてロボット調教師のサーバ証明書７５を失効させる場合には、ロボット調教師のシリアル「０ｘ００４９」）を実際に失効させるべきシリアルとしてサーバ証明書失効通知部１１２から入力し、サーバ証明書７５の失効を行う。

（１）　アプリケーションサーバのサーバ秘密鍵が暴露された

（２）　アプリケーションサーバの運用を停止した

（３）　アプリケーションサーバの名前を変更した

【００９５】

失効証明書検索部１１３は、サーバ証明書期限検索部１１１あるいはサーバ証明書失効通知部１１２から通知された失効させるべきシリアルと同じか、それより小さいシリアルをサーバ証明書履歴テーブル１１０ａの中すべて列挙し、証明書失効通知部１１４にその名前をすべて通知する。そして、失効証明書検索部１１３は、列挙したシリアルに対してサーバ証明書７５の更新がすべて終了した後に、失効させるべきシリアルの最大値に「１」加えたものに失効番号を更新し、失効番号蓄積部１１５に蓄積する。また、失効証明書検索部１１３は、列挙したシリアルに対してサーバ証明書７５の更新がすべて終了した後に、サーバ証明書履歴蓄積部１１０から列挙したシリアルのサーバ証明書７５に関する情報を削除する。

【００９６】

証明書失効通知部１１４は、失効証明書検索部１１３から通知された名前のアプリケーションサーバ３０ａ～３０ｋに対してサーバ証明書７５の更新要求を行う。アプリケーションサーバ３０ａ～３０ｋはサーバ証明書７５の更新要求に従ってサーバ証明書７５を更新する。この際、サーバ証明書送信部１０９は、更新されたサーバ証明書７５の送信を失効証明書検索部１１３に通知する。

【００９７】

失効番号蓄積部１１５は、サーバ証明書送信部１０９から発行されたサーバ証明書７５のシリアルの内、現在も有効な最も小さいシリアルを失効番号として蓄

積する。なお、失効番号の初期値は「０」である。失効番号蓄積部１１５に蓄積された失効番号は、失効情報署名部１１６に送られる。

【００９８】

失効情報署名部１１６は、失効情報９０に必要な発行者９１と、失効番号９２と、署名９３とで失効情報９０を組み立てて、失効情報通知部１１７に出力する。なお、署名９３は、ここでは発行者９１及び失効番号９２を連結したものをＣＡ秘密鍵蓄積部１０３に蓄積されたＣＡ秘密鍵で暗号化することで作成されている。

【００９９】

失効情報通知部１１７は、失効情報９０をリポジトリ２０に通知する。

リポジトリ２０は、失効情報蓄積部２０１と、通信部２０２とを備える。

【０１００】

リポジトリ２０の失効情報蓄積部２０１は、サーバ証明書作成装置１０から失効情報９０が送信されてくると、送信されてきた失効情報９０を失効情報蓄積部２０１に蓄積する。

【０１０１】

通信部２０２は、上述の暗号なしのプロトコル等に従ってインターネット５０を介して端末４０ａ～４０ｎと通信するインターフェースであり、端末４０ａ～４０ｎから失効情報９０配信のリクエストがあった場合、失効情報蓄積部２０１に蓄積されている失効情報９０をリクエストを発した端末４０ａ～４０ｎに送信する。このとき、通信は暗号化する必要はなく、またリポジトリのサーバ認証も必要がない。

【０１０２】

アプリケーションサーバ３０ａ～３０ｋは、鍵ペア作成部３０１と、ＣＳＲ作成部３０２と、サーバ秘密鍵蓄積部３０３と、サーバ証明書蓄積部３０４と、アプリサーバ部３０５と、通信部３０６とを備える。

【０１０３】

鍵ペア作成部３０１は、アプリケーションサーバ３０ａ～３０ｋ設置時に、ＲＳＡ暗号で暗号及び復号する時の鍵ペアであるサーバ公開鍵とサーバ秘密鍵を作

成する。

【０１０４】

ＣＳＲ作成部３０２は、認証局に対してサーバ証明書７５を作成させる時の雛形、すなわちサーバ公開鍵とサーバの名前を含むＣＳＲ７０を作成し、サーバ証明書作成装置１０に送付する。

【０１０５】

サーバ秘密鍵蓄積部３０３は、鍵ペア作成部３０１が作成したサーバ秘密鍵を蓄積する。

【０１０６】

サーバ証明書蓄積部３０４は、サーバ証明書作成装置１０から受信したサーバ証明書７５を蓄積する。

【０１０７】

なお、サーバ証明書作成装置１０からサーバ証明書７５の更新要求があった場合には、鍵ペア作成部３０１は新しいサーバ公開鍵及びサーバ秘密鍵を作成し、設置時と同様にＣＳＲ作成部３０２は新しいサーバ公開鍵でＣＳＲ７０を作成しサーバ証明書作成装置１０にサーバ証明書７５の作成を依頼し、サーバ証明書蓄積部３０４は新しいサーバ証明書７５をサーバ証明書作成装置１０から受け取り蓄積する。

【０１０８】

アプリサーバ部３０５は、通信部３０６を介して受信したリクエストを処理してレスポンスを作成し、作成したレスポンスを通信部３０６に出力する。

【０１０９】

通信部３０６は、上述の暗号化のためのプロトコル等に従ってインターネット５０を介して端末４０ａ～４０ｎと通信するインターフェースであり、端末４０ａ～４０ｎから送信されてきたリクエストやコマンドを解析したり、その結果に応じてサーバ認証のためにサーバ証明書７５をサーバ証明書蓄積部３０４から取り出し端末４０ａ～４０ｎに送信したり、端末４０ａ～４０ｎから受信した暗号の種類をサーバ秘密鍵蓄積部３０３に蓄積したサーバ秘密鍵で復号し、暗号化通信の共有鍵を作成したり、端末４０ａ～４０ｎから暗号化した通信でリクエスト

を受けた場合、リクエストを復号してアプリサーバ部３０５に出力したり、アプリサーバ部３０５から依頼されたレスポンスを暗号化して端末４０ａ～４０ｎに出力したりする。

【０１１０】

端末４０ａ～４０ｎは、アプリケーションサーバ３０ａ～３０ｋに対するリクエストを出力した、アプリケーションサーバ３０ａ～３０ｋからのレスポンスを受信するアプリクライアント部４１０と、通信部４２０と、上記リクエスト及びレスポンスの送受信の前にアプリケーションサーバ３０ａ～３０ｋから送られてくるサーバ証明書７５を検証するサーバ証明書検証部４３０とを備える。

【０１１１】

通信部４２０は、上述の暗号化あるいは非暗号のプロトコル等に従ってインターネット５０を介してアプリケーションサーバ３０ａ～３０ｋやリポジトリ２０と通信したりするインターフェースであり、アプリケーションサーバ３０ａ～３０ｋから送信されてきたコマンドを解析したり、その結果に応じてサーバ証明書検証部４３０に処理を依頼したり、アプリクライアント部４１０やサーバ証明書検証部４３０から渡されたデータをアプリケーションサーバ３０ａ～３０ｋに送信したり、サーバ証明書検証部４３０から渡されたデータをリポジトリ２０に送信したり、リポジトリ２０から失効情報９０を受信したりする。

【０１１２】

具体的には、通信部４２０は、通信部３０６に対して暗号化通信の開始を要求する。また、通信部４２０は、通信部３０６からサーバ証明書７５を受信し、受信したサーバ証明書７５をサーバ証明書検証部４３０に出力する。そして通信部４２０は、サーバ証明書検証部４３０からサーバ証明書７５の異常や失効を通知された場合、サーバ証明書７５の異常を通信部３０６に通知して通信を切断し、エラーをアプリクライアント部４１０に通知する。また、通信部４２０は、サーバ証明書７５の署名が正常であり、かつ、サーバ証明書７５が失効されていないときは、プリマスタシークレットを作成し、サーバ証明書７５に含まれるサーバ公開鍵を用いてプリマスタシークレットを暗号化して通信部３０６に送信する。また通信部４２０は、それまでの得たデータから暗号化通信の暗号鍵を作成する

。そして以降の通信において暗号鍵を用いた暗号化通信を行う。さらに、通信部４２０は、リポジトリ２０の通信部２０２に失効情報９０の配信を要求し、リポジトリ２０から受信した失効情報９０を署名検証部４３４に出力する。

【０１１３】

サーバ証明書検証部４３０は、失効情報要求部４３１と、署名検証部４３２と、ＣＡ証明書蓄積部４３３と、署名検証部４３４と、失効番号検証部４３５と、失効番号蓄積部４３６と、証明書シリアル抽出部４３７と、失効判定部４３８等とからなる。

【０１１４】

失効情報要求部４３１は、定期的にリポジトリ２０から失効情報９０を取得するよう通信部４２０に要求する。

【０１１５】

署名検証部４３２は、通信部４２０からサーバ証明書７５を受信すると、ＣＡ証明書蓄積部４３３からＣＡ公開鍵を取り出し、サーバ証明書７５の署名を検証し、署名が異常であれば通信部４２０に異常を通知する。

【０１１６】

ＣＡ証明書蓄積部４３３は、サーバ証明書作成装置１０から入手したＣＡ証明書６０を、予め蓄積する。

【０１１７】

署名検証部４３４は、通信部４２０から失効情報９０を受信すると、ＣＡ証明書蓄積部４３３からＣＡ公開鍵を取り出し、失効情報９０の署名の検証を行い、署名が正しければ失効番号を失効番号検証部４３５に出力する。

【０１１８】

失効番号検証部４３５は、失効番号蓄積部４３６から現在の失効番号を呼び出し、署名検証部４３４から入力された失効番号が現在の失効番号より大きい場合に限って入力された失効番号を新しい失効番号として失効番号蓄積部４３６に蓄積する。

【０１１９】

失効番号蓄積部４３６は、失効番号の初期値として「０」を予め記憶しており

、失効番号検証部４３５から失効番号が出力されるごとにその時点の最新の失効番号を更新しつつ蓄積する。

【０１２０】

証明書シリアル抽出部４３７は、入力されたサーバ証明書７５からシリアルを抽出し、失効判定部４３８に出力する。

【０１２１】

失効判定部４３８は、失効番号蓄積部４３６から失効番号を取り出し、抽出したシリアルと比較する。失効判定部４３８は抽出したシリアルが失効番号より小さい場合は、失効判定部４３８は、サーバ証明書７５が失効していることを通信部４２０に通知する。

【０１２２】

次いで、サーバ証明書作成装置１０、アプリケーションサーバ３０ａ～３０ｋ及び端末４０ａ～４０ｎの動作を詳述する。

【０１２３】

図５は、サーバ証明書組立部１０７が行う証明書用シリアル設定処理の動作を示すフローチャートである。

【０１２４】

サーバ証明書組立部１０７は、まずサーバ証明書７５に設定すべきシリアルＳｅの初期値として「０」を設定し（Ｓ１１）、ＣＳＲ受信部１０６を介してＣＳＲ７０を受信するのを待つ（Ｓ１２）。ＣＳＲ７０を受信すると（Ｓ１２でＹｅｓ）、サーバ証明書組立部１０７は、シリアル蓄積部１０５からシリアルＳｅを読み取り（Ｓ１３）、時計１０４から読み取った現在時刻やＣＳＲ７０等を用いてサーバ証明書を組み立て（Ｓ１４）、組み立てたサーバ証明書を署名部１０８に出力した後、シリアル蓄積部１０５に蓄積させるシリアルＳｅを「１」インクリメントし（Ｓ１５）、サーバ証明書の要部、名前、シリアル、有効期限をサーバ証明書履歴テーブル１１０ａに蓄積させる（Ｓ１６）。このような処理（Ｓ１２～Ｓ１６）を繰り返すことにより、シリアルが単調増加するサーバ証明書７５が順次発行されることになる。

【０１２５】

次いでサーバ証明書期限検索部１１１が行う証明書期限管理処理を説明する。

【０１２６】

図６は、サーバ証明書期限検索部１１１が行う証明書期限管理処理の動作を示すフローチャートである。なお、この処理は、所定の時間ごとに定期的に行われる。

【０１２７】

サーバ証明書期限検索部１１１は、まずサーバ証明書履歴テーブル１１０ａのシリアルをサーチし、サーバ証明書履歴テーブル１１０ａに格納されているシリアルの最小値Ｓｅｍｉｎ及びシリアルの最大値Ｓｅｍａｘを取得し、有効期限の到来が早いシリアル、すなわちシリアルの最小値Ｓｅｍｉｎをセットする（Ｓ２１）。そして、サーバ証明書期限検索部１１１は、そのシリアルについて１月以内に有効期限が到来するか否か判断する（Ｓ２２）。判断の結果到来する場合には（Ｓ２２でＹｅｓ）、サーバ証明書期限検索部１１１は、そのシリアルを実際に失効させるべきシリアルの最大値Ｓｅｅｎｄにセットし、次のレコードの有効期限をサーチするためにシリアルＳｅを「１」インクリメントする（Ｓ２３）。シリアルＳｅのインクリメントが終わると、サーバ証明書期限検索部１１１は、サーバ証明書履歴テーブル１１０ａの最後のレコードのシリアルＳｅｍａｘまですべて有効期限の到来をみたか判断する（Ｓ２４）。最後のレコードまでみていなければ（Ｓ２４でＮｏ）、サーバ証明書期限検索部１１１は、ステップＳ２２～Ｓ２４を繰り返し実行し、実際に失効させるべきシリアルの最大値Ｓｅｅｎｄを順次取得する。

【０１２８】

判断の結果１月以内に有効期限が到来しない場合（Ｓ２２でＮｏ）、あるいは最後のレコードまでみた場合（Ｓ２４でＹｅｓ）には、サーバ証明書期限検索部１１１は、実際に失効させるべきシリアルの最大値Ｓｅｅｎｄを失効証明書検索部１１３に通知する（Ｓ２５）。

【０１２９】

このような処理を繰り返すことにより有効期限が到来するサーバ証明書７５のシリアルが時々刻々失効証明書検索部１１３に通知される。

【０１３０】

次いで、失効証明書検索部１１３が行う有効期限到来による失効証明書検索処理を説明する。

【０１３１】

図７は、失効証明書検索部１１３が有効期限到来による失効証明書検索処理の動作を示すフローチャートである。なお、この処理は、所定の時間ごとに定期的に行われる。

【０１３２】

失効証明書検索部１１３は、サーバ証明書期限検索部１１１から実際に失効させるべきシリアルの最大値Ｓｅｅｎｄの通知がくるのを待つ（Ｓ３１）。実際に失効させるべきシリアルの最大値Ｓｅｅｎｄの通知がくると（Ｓ３１でＹｅｓ）、失効証明書検索部１１３は、サーバ証明書履歴テーブル１１０ａの最小のシリアルＳｅｍｉｎからこのシリアルの最大値Ｓｅｅｎｄまでのシリアルに対応するサーバの名前を証明書失効通知部１１４に通知する（Ｓ３２）。これにより、証明書失効通知部１１４から各アプリケーションサーバ３０ａ～３０ｋに失効通知８０が送られ、この失効通知８０を受けたアプリケーションサーバ３０ａ～３０ｋがＣＳＲ７０を送信し、これらのアプリケーションサーバ３０ａ～３０ｋに単調に増加するシリアルが付されたサーバ証明書７５が順次新たに発行されることになる。

【０１３３】

そして、失効証明書検索部１１３は、シリアルの値が増加された新たなサーバ証明書が全て発行されるのを待つ（Ｓ３３）。

【０１３４】

サーバ証明書７５を発行し終わると（Ｓ３３でＹｅｓ）、失効証明書検索部１１３は、シリアルＳｅｍｉｎ～Ｓｅｅｎｄのレコードを全て削除し（Ｓ３４）、実際に失効させるべきシリアルの最大値Ｓｅｅｎｄに「１」加えた値を失効シリアルとして失効番号蓄積部１１５に格納する（Ｓ３２）。

【０１３５】

このような処理を繰り返すことにより、有効期限を迎えるサーバ証明書７５は

順次失効の対処とされ、この失効の対象とされたサーバ証明書７５を有するアプリケーションサーバ３０ａ～３０ｋはシリアル番号が増加された新たなサーバ証明書７５に更新することになる。

【０１３６】

次いで、失効証明書検索部１１３が行うサーバ証明書失効通知部１１２からの失効通知による失効検索処理を説明する。

【０１３７】

図８は、失効証明書検索部１１３が行う失効通知による失効証明書検索処理の動作を示すフローチャートである。なお、この処理は、所定の時間ごとに定期的に行われる。

【０１３８】

失効証明書検索部１１３は、サーバ証明書失効通知部１１２から失効通知がくるのを待つ（Ｓ４１）。失効通知があると、失効証明書検索部１１３は、通知されたシリアルＳｅを特定し（Ｓ４２）、サーバ証明書履歴テーブル１１０ａの最小のシリアルＳｅｍｉｎからこの特定されたシリアルＳｅまでのシリアルに対応するサーバの名前を証明書失効通知部１１４に通知する（Ｓ４３）。これにより、証明書失効通知部１１４から各アプリケーションサーバ３０ａ～３０ｋに失効通知８０が送られ、この失効通知８０を受けたアプリケーションサーバ３０ａ～３０ｋがＣＳＲ７０を送信し、これらのアプリケーションサーバ３０ａ～３０ｋに単調に増加するシリアルが付されたサーバ証明書７５が順次新たに発行されることになる。

【０１３９】

そして、失効証明書検索部１１３は、新たにサーバ証明書が全て発行されるのを待つ（Ｓ４４）。

【０１４０】

サーバ証明書７５を発行し終わると（Ｓ４４でＹｅｓ）、失効証明書検索部１１３は、シリアルＳｅｍｉｎ～特定したシリアルＳｅのレコードを全て削除し（Ｓ４５）、実際に失効させるべき特定されたシリアルＳｅに「１」加えた値を失効シリアルとして失効番号蓄積部１１５に格納する（Ｓ４６）。

【０１４１】

このような処理を繰り返すことにより、失効の対象とされたサーバ証明書７５のみならずこれより小さな値のシリアルが付されたサーバ証明書７５は全て失効の対処とされ、この失効の対象とされたサーバ証明書７５を有するアプリケーションサーバ３０ａ～３０ｋはシリアル番号が増加された新たなサーバ証明書７５に更新することになる。

【０１４２】

次いで、失効情報署名部１１６が行う失効情報組立処理を説明する。

【０１４３】

図９は、失効情報署名部１１６が行う失効情報組立処理の動作を示すフローチャートである。

【０１４４】

失効情報署名部１１６は、失効番号蓄積部１１５から失効シリアルＳｅの初期値「0」をセットする（Ｓ５１）。そして、この失効シリアルＳｅと、予め保持している発行者と、ＣＡ秘密鍵蓄積部１０３から読み出したＣＡ秘密鍵を用いて形成する署名とで失効情報９０を組み立てて、失効情報通知部１１７に出力する。

【０１４５】

次いで、失効情報署名部１１６は、失効番号蓄積部１１５をモニタし、失効シリアルが失効シリアル変化するのをまつ（Ｓ５２）。ここで、失効シリアルから「1」減算した値のシリアル以下のサーバ証明書７５は全て失効の対象とされている。このため、このステップＳ５２での実際の判断は、失効シリアルが増加したか否かの判断でたりる。失効シリアルが増加すると、失効情報署名部１１６は、変化後の失効シリアルＳｅを失効番号蓄積部１１５から読み取り（Ｓ５３）、この失効シリアルＳｅと、予め保持している発行者と、ＣＡ秘密鍵蓄積部１０３から読み出したＣＡ秘密鍵を用いて形成する署名とで失効情報９０を組み立てて（Ｓ５４）、失効情報通知部１１７に出力する。

【０１４６】

このような処理を繰り返すことにより、リポジトリ２０の失効情報蓄積部２０

１には、失効シリアルの値が増加する失効情報９０が順次蓄積されることになる。

【０１４７】

次いで、端末４０ａ～４０ｎのサーバ証明書検証部４３０が行う失効情報取得処理を説明する。

【０１４８】

図１０は、サーバ証明書検証部４３０の各部が行う失効情報取得処理の動作を示すフローチャートである。なお、この処理は、所定の時間（１月に１回）ごとに定期的に行われる。

【０１４９】

各端末４０ａ～４０ｎの失効情報要求部４３１は、先ず、リポジトリ２０から失効情報９０を定期的（１月に１回）に入手して、失効番号を蓄積する。具体的には、失効情報要求部４３１は、内部タイマーによる計時で１月経過するのを待ち（Ｓ６１）、１月経過すると（Ｓ６１でＹｅｓ）、リポジトリ２０に対して失効情報の配信を要求し（Ｓ６２）、失効情報９０が配信されるのを待つ（Ｓ６３）。

【０１５０】

このとき、入手した失効情報９０が偽である場合の失効番号を蓄積すると、正規のアプリケーションサーバを不正であると判断したり、不正なアプリケーションサーバを正規とみなしたりするので、次のチェックを行う。

【０１５１】

すなわち、失効情報９０が送られてくると（Ｓ６２でＹｅｓ）、まず最初に署名検証部４３４は、失効情報９０の署名が正しいかを確認する（Ｓ６４）。失効情報９０の署名はサーバ証明書作成装置１０しか行えないため、署名が正しければそれは正しいデータとする。

【０１５２】

次に、失効番号が現在蓄積しているより大きな番号であることを確認する。具体的には、失効番号検証部４３５は、配信された失効シリアルを取得し（Ｓ６５）、配信された失効シリアルの値が失効番号蓄積部４３６に蓄積している失効シ

リアルの値より大きいか否かを判断する（Ｓ６６）。失効番号は、サーバ証明書７５の失効により単調増加され、減少することがない。

【０１５３】

したがって、受信した失効情報９０の失効番号が現在保持している失効番号より大きい番号であれば（Ｓ６６でＹｅｓ）、配信された失効シリアルを蓄積する（Ｓ６７）。これに対してし、現在の失効番号より小さな番号であれば（Ｓ６６でＮｏ）、それは偽の失効番号であるか、なにかの手違いであると推定し、失効情報を廃棄する（Ｓ６８）。

【０１５４】

このような処理を繰り返し行うことにより、サーバ証明書検証部４３０は値が単調に増加する正規の失効番号だけを蓄積することができる。

【０１５５】

次に端末４０ａ～４０ｎ及びアプリケーションサーバ３０ａ～３０ｋ間で暗号化して通信を行う場合について説明する。

【０１５６】

図１１は、暗号化して通信を行う場合のシーケンス図である。なおここでは、端末４０ａとアプリケーションサーバ３０ａとの間で行われた場合をその代表例として説明する。

【０１５７】

端末４０ａのアプリクライアント部４１０は、暗号化してアプリケーションサーバ３０ａにリクエスト３を送るよう通信部４２０に指示を行う（Ｓ１００）。通信部４２０は、クライアント乱数と通信部４２０が処理できる暗号の種類を含んだＣｌｉｅｎｔＨｅｌｌｏパケットをアプリケーションサーバ３０ａの通信部３０６に送信し、ＳＳＬのハンドシェークを開始する（Ｓ１０１）。

【０１５８】

アプリケーションサーバ３０ａの通信部３０６は、ＣｌｉｅｎｔＨｅｌｌｏパケットから暗号の種類を決定し、サーバ乱数とセッションＩＤとともにＳｅｒｖｅｒｈｅｌｌｏパケットで暗号の種類を送り（Ｓ１０２）、サーバ証明書蓄積部３０４からサーバ証明書７５を取り出し（Ｓ１０３）、サーバ証明書７５をＣｅ

ｒｔｉｆｉｃａｔｅパケットとしてアプリケーションサーバ３０ａの通信部４２０に送信し（Ｓ１０４）、さらにＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅパケットを通信部４２０に送る（Ｓ１０７）。

【０１５９】

端末４０ａの通信部４２０は、Ｃｅｒｔｉｆｉｃａｔｅパケットからサーバ証明書７５を取り出し、サーバ証明書検証部４３０に送る（Ｓ１０５）。サーバ証明書検証部４３０は、サーバ証明書７５が不正でないか検証し、検証結果を通信部３０６に通知する（Ｓ１０６）。サーバ証明書７５が不正であれば、通信部４２０は、アラートパケットを通信部３０６に送信して通信を切断し、アプリクライアント部４１０にエラーを返す。これに対して、サーバ証明書７５が不正でない場合には、通信部４２０は、暗号化の共有鍵を計算するためのプリマスターシークレットを作成し、サーバ証明書７５に含まれるサーバ公開鍵で暗号化し、ＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅパケットの到着後に暗号化されたプリマスターシークレットを含むＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅパケットを通信部３０６に送信し（Ｓ１０８）、ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃパケットを通信部３０６に送信する（Ｓ１０９）。ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃパケットは暗号化の開始を示すパケットである。通信部４２０は、クライアント乱数とサーバ乱数とプリマスターシークレットから暗号化に使用する共通鍵Ａを作成し、ハンドシェークの終了を示すＦｉｎｉｓｈｅｄパケットを作成した共通鍵Ａで暗号化してアプリケーションサーバ３０ａの通信部３０６に送信する（Ｓ１１０）。

【０１６０】

アプリケーションサーバ３０ａの通信部３０６は、ＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅから暗号化されたプリマスターシークレットを取り出し、サーバ秘密鍵を用いてプリマスターシークレットに復号し、サーバ乱数、クライアント乱数とともに暗号化に使用する共通鍵Ｂを作成する。ＳＳＬのハンドシェークが正常に行われた場合、通信部３０６の持つ共通鍵Ａと通信部４２０の持つ共通鍵Ｂは同一となる。通信部３０６は、受信したＦｉｎｉｓｈｅｄパケットを共通鍵Ｂで復号し、正常に復号できればＦｉｎｉｓｈパケットを暗号化して通信部４２０に送付する（Ｓ１１１）。このＦｉｎｉｓｈパケット以降の通信は、すべて暗号化

して行われる。

【０１６１】

端末４０ａの通信部４２０は、受信したＦｉｎｉｓｈｅｄパケットを復号し、正常に復号できれば、リクエスト３を暗号化してアプリケーションサーバ３０ａの通信部３０６に送付する（Ｓ１１２）。

【０１６２】

アプリケーションサーバ３０ａの通信部３０６は、リクエスト３を復号し、アプリサーバ部３０５に送る（Ｓ１１３）。アプリサーバ部３０５は、リクエスト３を処理してレスポンス３を生成し、端末４０ａ～４０ｎに送るよう通信部３０６に指示する（Ｓ１１４）。通信部３０６は、端末４０ａの通信部４２０にレスポンス３を暗号化して送信する（Ｓ１１５）。

【０１６３】

端末４０ａの通信部４２０は、レスポンス３を復号してアプリクライアント部４１０に送付する（Ｓ１１６）。

【０１６４】

以上のように暗号化を行い通信する。

【０１６５】

次いで、サーバ証明書検証部４３０が行う検証について説明する。

【０１６６】

図１２は、サーバ証明書検証部４３０が行うサーバ証明書７５の検証動作を示すフローチャートである。

【０１６７】

サーバ証明書検証部４３０の署名検証部４３２は、サーバ証明書７５を取得すると、取得したサーバ証明書７５から発行者を取り出し、ＣＡ証明書蓄積部４３３から、その発行者のＣＡ証明書６０を検索する。そして、ＣＡ証明書６０からＣＡの公開鍵を取り出し、ＣＡの公開鍵を用いてサーバ証明書７５の署名のチェックをする。具体的には、署名検証部４３２は、サーバ証明書７５が配信されてくるのを待ち（Ｓ８１）、配信されてくると（Ｓ８１でＹｅｓ）、サーバ証明書７５の発行者を取得し（Ｓ８２）、発行者が同一のＣＡ証明書６０をＣＡ証明書

蓄積部４３３から検索する（Ｓ８３）。そして、署名検証部４３２は、検索によって得られたＣＡ証明書６０のＣＡ公開鍵を取り出し（Ｓ８４）、公開鍵で復号化することによりサーバ証明書の署名が正しいか否か判断する（Ｓ８５）。

【０１６８】

チェックの結果、サーバ証明書７５の署名が不正であれば（Ｓ８５で署名ＮＧ）、署名の検証エラーのエラーコードを通信部４２０に通知して（Ｓ９０）、検証を終了する。これに対して、署名が正しければ（Ｓ８５で署名ＯＫ）、証明書シリアル抽出部４３７は、サーバ証明書７５からシリアル（サーバシリアル）を取り出す（Ｓ８６）。そして、失効判定部４３８は、失効番号蓄積部４３６から失効番号を取り出し、証明書シリアル抽出部４３７が取り出したシリアルと比較する。すなわち、サーバシリアルと失効シリアルとの大小関係を判断する（Ｓ８８）。

【０１６９】

もしシリアルが失効番号より小さければ（Ｓ８８でＮｏ）、失効判定部４３８は、そのサーバ証明書７５が失効していると判断し、失効のエラーコードを通信部４２０に通知して（Ｓ９０）、検証を終了する。これに対して、もしシリアルが失効番号より大きいか同じであれば（Ｓ８８でＹｅｓ）、失効判定部４３８は、そのサーバ証明書７５は正しいと判断して、通信部４２０に正常終了を通知する。

【０１７０】

このような処理により署名が正当で、しかも失効番号以上の値のシリアルを含むサーバ証明書７５をアプリケーションサーバ３０ａが送った場合にだけ認証される。

【０１７１】

ここで、サーバ証明書作成装置１０が作成するサーバ証明書７５のシリアルと失効番号の関係について説明する。

【０１７２】

図１３は、サーバが４台あったときのサーバ証明書７５のシリアルと失効番号との関係を示す図である。

【０１７３】

なお、ここではサーバをＡ，Ｂ，Ｃ，Ｄとし、サーバはそれぞれ時刻「ａ」，「ｂ」，「ｃ」，「ｄ」に設置されるものとし、各サーバが保持するサーバ証明書７５のシリアルはそれぞれ「０」，「１」，「２」，「３」であるものとして説明する。

【０１７４】

時刻「ｅ」にサーバＣのサーバ証明書７５の安全性が危惧された場合、この時点におけるサーバ証明書履歴蓄積部１１０に蓄積されている情報は次のとおりである。

【０１７５】

サーバ名	シリアル	有効期限
Ａ	０	ａ＋１３（ヶ月）
Ｂ	１	ｂ＋１３（ヶ月）
Ｃ	２	ｃ＋１３（ヶ月）
Ｄ	３	ｄ＋１３（ヶ月）

したがって、サーバ証明書作成装置１０の失効証明書検索部１１３は、サーバＣのサーバ証明書７５のシリアル「２」より小さなシリアルをもつサーバ証明書７５を検索する。結果はサーバＡ及びサーバＢのサーバ証明書７５である。従って、サーバ証明書作成装置１０の証明書失効通知部１１４は、サーバＡ，Ｂ，Ｃに対してサーバ証明書７５の更新要求（サーバ証明書７５の失効通知）を行う。その結果サーバＡ，Ｂ，Ｃから新しいサーバ証明書７５の作成要求があり、それぞれシリアルが「４」、「５」，「６」であるサーバ証明書７５を新規に作成し、各アプリケーションサーバＡ～Ｃに返送する。このとき作成したサーバ証明書７５の有効期限はｅ＋１３ヶ月とする。また同時にサーバ証明書履歴蓄積部１１０のデータは

サーバ名	シリアル	有効期限
Ｄ	３	ｄ＋１３（ヶ月）
Ａ	４	ｅ＋１３（ヶ月）
Ｂ	５	ｅ＋１３（ヶ月）

Ｃ　：　６　：　ｅ＋１３（ヶ月）

に更新される。

【０１７６】

サーバ証明書作成装置１０の失効番号蓄積部１１５は、各サーバのサーバ証明書７５が更新された後に失効番号をその時点で有効かつ最小のシリアル「３」に変更し、このシリアルを含む失効情報９０をリポジトリ２０の失効情報蓄積部２０１に蓄積させる。すなわち、新しい失効番号は、失効原因となったサーバＣの元のサーバ証明書７５のシリアル「２」に「１」を加えた値である「３」である。

【０１７７】

端末４０ａ～４０ｎは、リポジトリ２０から失効番号を定期的に入手して蓄積する。このとき偽の失効番号を蓄積すると、正規のサーバを不正であると判断したり、不正なサーバを正規にみなしたりするので次のチェックを行う。まず最初に失効情報の署名を確認する。失効情報の署名はＣＡにしか署名できないため署名が正しければそれは正しいデータとする。次に失効番号が現在蓄積しているより大きな番号であることを確認する。失効番号はサーバ証明書の失効により増加を行うが、減少はしないので現在の失効番号より小さな番号であればそれは偽の失効番号であるか、なにかの手違いであると推定し、それを廃棄する。

【０１７８】

ところで、サーバＣのサーバ証明書７５を用いてサーバの成りすましがあったとした場合、なりすましたサーバのサーバ証明書７５のシリアルは「２」であり、その時点で端末の失効番号は「３」であるため、失効番号より小さなシリアルを持つサーバ証明書７５は失効されているという条件に合致し、そのサーバを信用することはない。

【０１７９】

また、サーバ証明書期限検索部１１１は、常にサーバ証明書履歴蓄積部１１０を検索し、現在時刻より１ヶ月内に有効期限がくるサーバ証明書７５を検索する。例えばｄ＋１２ヶ月を過ぎれば、サーバＤのサーバ証明書７５の期限が１ヶ月内となる。このときサーバ証明書期限検索部１１１は、サーバＤが保持するサー

バ証明書７５のシリアル「３」を失効証明書検索部１１３に通知し、証明書失効通知部１１４はサーバＤに対してサーバ証明書７５の更新を要求する。またサーバＤのサーバ証明書７５のシリアルより小さなシリアルを持つサーバ証明書７５を持つサーバがあれば、そのサーバに対してもサーバ証明書７５の更新要求を行う。そしてこれらのサーバ証明書７５の更新が終わったあとで失効番号をサーバＤのサーバ証明書７５のシリアルに「１」を加えた「４」に更新する。

【０１８０】

このように有効期限が近づいたサーバ証明書７５を更新するときに、有効期限の近づいたサーバ証明書７５が持つシリアルより小さいシリアルをもつサーバ証明書７５を全て更新し、期限の近づいたサーバ証明書７５のシリアルに「１」加えたものをあらたな失効番号とすることにより、有効期限が切れたサーバ証明書７５によってサーバが成りすまされた場合でも、時計がなく期限が正確に判断できない機器でも失効番号によってそのサーバ証明書７５の失効を確認できる。

【０１８１】

なお、ここでは更新後のシリアルをサーバＡ，Ｂ，Ｃの順で「４」，「５」，「６」としたが、特にこの順でなくともよい。

【０１８２】

なお、本実施の形態１では、シリアルの初期値を「０」とし、サーバ証明書７５の発行毎に「１」増加させたが、初期値は自由に設定でき、増加する値も単調増加する範囲において発行毎に異なっていてもよい。

【０１８３】

また、本実施の形態１では、失効番号の初期値を「０」としたが、シリアルの初期値以下の小さい値であれば、なんでもよい。つまり、例えばサーバ証明書７５のシリアルの初期値を「１」とした場合、失効番号の初期値を「０」としてもよく、「１」としてもよい。

【０１８４】

また、サーバ証明書７５のシリアルの初期値が失効番号の初期値以上の値に設定された状態で単調増加するシリアルのサーバ証明書７５が発行されるので、失効シリアルを参照したのと同等の機能が確保されるため、この実施の形態では参

照しなかったが、失効番号を実際に参照して失効番号以上のシリアルのサーバ証明書７５を発行するようにしてもよい。

【０１８５】

以上のように、本実施の形態１によれば、有効期限が切れそうなサーバ証明書を保持するアプリケーションサーバに対して失効通知を送り、新たなサーバ証明書を発行し、もとのサーバ証明書を失効させて使えなくなるようにしている。したがって、端末４０ａ～４０ｎは、有効期間をチェックする必要がなく、正確な時計を持つ必要もなくなる。また、失効情報９０には１つの失効シリアルだけが記録され、端末４０ａ～４０ｎはこれを記憶し、サーバ証明書７５のシリアルと失効番号との大小関係でサーバ証明書７５の有効性を判断するので、従来のようなリソースを用意する必要もなく、簡単なリソースでたり、ネット家電等にも適用できる。

【０１８６】

（実施の形態２）

以下、本発明の実施の形態２に係る通信システムついて説明する。

【０１８７】

図１４は、本発明の実施の形態２に係る通信システム２の全体構成を示すブロック図である。なお、図１に示される通信システム１の構成と同じ構成部分に同じ番号を付し、その説明を省略する。

【０１８８】

この通信システム２は、実施の形態１の通信システム１と同様、認証局が使用するサーバ証明書作成装置１１及びリポジトリ２１と、映像コンテンツなどのアプリケーション提供者が使用する複数のアプリケーションサーバ３０ａ～３０ｋと、ユーザが使用する複数の端末４１ａ～４１ｎと、リポジトリ２１、アプリケーションサーバ３０ａ～３０ｋ及び端末４１ａ～４１ｎを接続するインターネット５０とから構成される。

【０１８９】

ところで、実施の形態１の通信システム１は、サーバ証明書作成装置１０からリポジトリ２０に失効情報９０を送信し、リポジトリ２０から端末４０ａ～４０

ｎに失効情報９０を送信するように構成されている。これに対して実施の形態２の通信システム２は、サーバ証明書作成装置１１からリポジトリ２１には失効番号だけで構成される失効情報９０ｂを送信するように構成されており、この点が通信システム１の構成と大きく異なっている。

【０１９０】

また、通信システム１では、リポジトリ２０から各端末４０ａ～４０ｎに失効情報９０を暗号なしで送信し、各端末において失効情報９０の署名でその失効情報のすり替えをチェックするように構成されている。これに対して通信システム２は、リポジトリ２１がは、サーバ証明書作成装置１１からリポジトリ２１にサーバ証明書７５を発行し、リポジトリ２１は、端末４１ａ～４１ｎから失効番号配信の要求がくると、アプリケーションサーバ３０ａ～３０ｋの場合と同様、サーバ証明書７５を送信し、端末４０ａ～４０ｎからサーバ認証を受け、ＳＳＬによるセッション鍵を共有した後、失効番号を暗号化して配信するように構成されており、この点が通信システム１の構成と大きく異なっている。

【０１９１】

このため、サーバ証明書作成装置１１は、アプリケーションサーバ３０ａ～３０ｋの場合と同様、鍵ペア作成部１０１、ＣＡ証明書作成部１０２、ＣＡ秘密鍵蓄積部１０３、時計１０４、シリアル蓄積部１０５、ＣＳＲ受信部１０６、サーバ証明書組立部１０７、署名部１０８、サーバ証明書送信部１０９、サーバ証明書履歴蓄積部１１０、サーバ証明書期限検索部１１１、サーバ証明書失効通知部１１２、失効証明書検索部１１３、証明書失効通知部１１４を備え、リポジトリ２１から送られてきたＣＳＲ７０を受け付けて、リポジトリ２１にサーバ証明書７５を発行したり、このサーバ証明書７５が失効の対象となった場合にリポジトリ２１に失効通知８０を送信したりするように構成されている。しかも、サーバ証明書作成装置１１は、サーバ証明書作成装置１０で用いられていた失効情報署名部１１６が削除され、失効番号蓄積部１１５に代えて失効番号蓄積部１２１を、失効情報通知部１１７に代えて失効番号通知部１２２を備えて構成される。この失効番号蓄積部１２１は失効番号蓄積部１１５と同様に、サーバ証明書送信部１０９から発行されたサーバ証明書７５のシリアルの内、現在も有効な最も小さ

いシリアルを失効番号として蓄積する。なお、失効番号の初期値は「０」である。失効番号通知部１２２に蓄積された失効番号は、失効情報署名部１１６に送られる。失効番号通知部１２２は、失効番号蓄積部１２１に蓄積されている署名なしの失効番号だけを失効情報９０ｂとしてリポジトリ２１に通知する。

【０１９２】

リポジトリ２１は、鍵ペア作成部２０３と、ＣＳＲ７０作成部２０４と、サーバ秘密鍵蓄積部２０５と、サーバ証明書蓄積部２０７と、失効情報蓄積部２０８と、通信部２０９とを備える。

【０１９３】

リポジトリ２１は、アプリケーションサーバ３０ａ～３０ｋと同様に、端末４１ａ～４１ｎとの通信をＳＳＬを用いて行う。このため、鍵ペア作成部２０３は、設置時やサーバ証明書作成装置１１から失効通知８０を受信するごとに、サーバ公開鍵とサーバ秘密鍵を新たに作成する。サーバ公開鍵はＣＳＲ７０作成部２０４に送られ、サーバ秘密鍵はサーバ秘密鍵蓄積部２０５に蓄積される。

【０１９４】

ＣＳＲ７０作成部２０４は、サーバ公開鍵と予め保持するサーバの名前からＣＳＲ７０を作成し、サーバ証明書作成装置１１に送信する。これによって、サーバ証明書作成装置１１は、受信したＣＳＲ７０からサーバ証明書７５を作成し、作成したサーバ証明書７５をリポジトリ２１に送信する。サーバ証明書蓄積部２０７は、サーバ証明書７５を受信するごとに、受信した新しいサーバ証明書７５を蓄積する。

【０１９５】

失効情報蓄積部２０８は、サーバ証明書作成装置１１から失効番号だけで構成された失効情報９０ｂを受信するごとに、新しい失効番号を蓄積する。

【０１９６】

通信部２０９は、上述の暗号化のためのプロトコル等に従ってインターネット５０を介して端末４１ａ～４１ｎと通信するインターフェースである。具体的には、通信部２０９は、端末４１ａ～４１ｎから通信の開始要求を受けたとき、通信部３０６と同様、サーバ認証のためにサーバ証明書７５をサーバ証明書蓄積部

２０７から取り出し、端末４１ａ～４１ｎに送る。また通信部２０９は、端末４１ａ～４１ｎから受信した暗号の種類をサーバ秘密鍵蓄積部２０５に蓄積したサーバ秘密鍵で復号し、暗号化通信の共有鍵を作成する。その後通信部２０９は、端末４１ａ～４１ｎから暗号化した通信で失効番号のリクエストを受けた場合、失効情報蓄積部２０８から失効情報９０ｂを取り出し、失効情報９０ｂを暗号化して端末４１ａ～４１ｎに出力する。これに対して、暗号化しない通信でリクエストを受けた場合、通信部２０９は、通信を切断する。

【０１９７】

端末４１ａ～４１ｎは、アプリクライアント部４１０と、通信部４２０に代えて用いられる通信部４４０と、サーバ証明書検証部４３０に代えて用いられるサーバ証明書検証部４５０とから構成される。サーバ証明書検証部４５０は、サーバ証明書検証部４３０と同様、署名検証部４３２、ＣＡ証明書蓄積部４３３、失効番号蓄積部４３６、失効判定部４３８を備えるほか、失効情報要求部４３１に代えて用いられる失効情報要求部４５１と、証明書シリアル抽出部４３７に代えて用いられる証明書シリアル抽出部４５２と、失効番号検証部４３５に代えて用いられる失効番号検証部４５３とから構成される。

【０１９８】

端末４１ａ～４１ｎの失効情報要求部４５１は、定期的（例えば、１月に１回）にリポジトリ２１から失効番号を取得するよう通信部４４０に要求する。

【０１９９】

署名検証部４３２は、ＣＡ証明書蓄積部４３３からＣＡ証明書６０を取り出し、サーバ証明書７５の署名を検証し、署名が異常であれば通信部４４０に異常を通知する。

【０２００】

証明書シリアル抽出部４５２は、入力されたサーバ証明書７５からシリアルを抽出し、抽出したシリアルを失効判定部４３８と失効番号検証部４５３に出力する。

【０２０１】

失効番号検証部４５３は、失効番号蓄積部４３６に蓄積されている失効番号を

取り出し、リポジトリ２１から取得したシリアル（失効番号）と比較したり、証明書シリアル抽出部４５２から出力されたシリアルと比較する。そして、リポジトリ２１から取得したシリアルが失効番号蓄積部４３６に蓄積されている失効番号より小さい場合は、失効番号検証部４５３は、何らかの原因で異常であることを通信部４４０に通知する。また、失効番号検証部４５３は、アプリケーションサーバ３０ａ～３０ｋやリポジトリ２１から抽出したサーバ証明書７５のシリアルが失効番号より小さい場合は、サーバ証明書７５が失効していることを通信部４４０に通知する。

【０２０２】

通信部４４０は、上述の暗号化あるいは非暗号のプロトコル等に従ってインターネット５０を介してアプリケーションサーバ３０ａ～３０ｋやリポジトリ２１と通信したりするインターフェースであり、通信部４２０と同様にアプリケーションサーバ３０ａ～３０ｋと通信するほか、リポジトリ２１から送信されてきたコマンドを解析したり、その結果に応じてサーバ証明書検証部４３０に処理を依頼したり、アプリクライアント部４１０やサーバ証明書検証部４５０から渡されたデータをリポジトリ２１に送信したり、リポジトリ２１からサーバ証明書７５及び失効情報９０を受信したりする。つまり、通信部４４０は、図１１に示される通信プロトコルを用いて失効情報９０ｂを暗号化通信する。

【０２０３】

具体的には、通信部４４０は、失効情報要求部４５１からの失効情報９０ｂの要求があると、リポジトリ２１の通信部２０９に対して暗号化通信の開始を要求する。これにより、通信部４４０には、リポジトリ２１の通信部２０９よりサーバ証明書７５が通知される。

【０２０４】

通信部４４０は、受信したサーバ証明書７５を、署名検証部４３２と、証明書シリアル抽出部４５２に出力する。この出力の結果署名検証部４３２から異常を通知された場合、通信部４４０は、サーバ証明書７５の異常をリポジトリ２１の通信部２０９に通知して通信を切断する。

【０２０５】

サーバ証明書７５の署名が正常であり、サーバ証明書７５が失効されていないときは、通信部４４０は、プリマスタシークレットを作成し、サーバ証明書７５に含まれるサーバ公開鍵を用いてプリマスタシークレットを暗号化してリポジトリ２１の通信部２０９に送信する。そして、通信部４４０は、それまでに得たデータから暗号化通信の暗号鍵を作成する。そして以降の通信において暗号鍵を用いた暗号化通信を行う。つまり、通信部４４０は、失効番号のリクエストをリポジトリ２１に暗号化して送信する。リポジトリ２１から暗号化された失効情報９０ｂ（失効番号）を受信すると、通信部４４０は、受信した暗号化された失効番号を復号し、失効番号検証部４５３に出力する。

【０２０６】

失効番号検証部４５３は、失効番号蓄積部４３６から現在の失効番号を読み出し、リポジトリ２１から通知された失効番号と比較する。このとき現在の失効番号より通知された失効番号が小さければ通知された失効番号は無効と判断し、処理を終了する。なぜならば、失効番号は単調増加するので、現在の失効番号より小さな失効番号に変更されることはありえないからである。また、現在の失効番号と通知された失効番号が同じ場合には、変更がなかったとして処理を終了する。現在の失効番号より通知された失効番号が大きい場合には、失効番号検証部４５３は、通知された失効番号と証明書シリアル抽出部４５２から入力されるリポジトリ２１のシリアルを比較する。失効番号検証部４５３は、通知された失効番号がリポジトリ２１のシリアルより小さければ通知された失効番号は無効と判断し処理を終了する。なぜならば、通知された失効番号を有効と仮定すれば、リポジトリ２１のシリアルが無効、すなわちサーバ証明書７５が失効しているということになり、無効なサーバ証明書７５を持つリポジトリ２１から取得した失効番号が信用できないためである。失効番号検証部４５３は、通知された失効番号がリポジトリ２１のシリアルより大きいか同じであれば、通知された失効番号を新たな失効番号として失効番号蓄積部４３６に蓄積する。

【０２０７】

なお、失効番号に対する攻撃として、失効番号を小さくして過去に脆弱となったサーバ証明書７５を有効にする攻撃と、失効番号を大きくしてオーバフローさ

せる攻撃が考えられるが、これらに対するために以上のような失効番号の有効性の判定を行う。

【０２０８】

以上のようにすることで、失効情報９０ｂの入手の際に署名のチェックを行わなくてもよく、正常な失効番号だけを保持することができる。

【０２０９】

なお、本発明の他の実施の形態として、発明の構成を、以下のようにしてもよい。

【０２１０】

証明書発行装置は、失効番号を蓄積する失効番号蓄積手段と、過去に発行したサーバ証明書の識別番号と期限と発行先を蓄積するサーバ証明書情報蓄積手段と、新たにサーバ証明書を発行する証明書発行手段を持ち、新たにサーバ証明書を発行する場合には失効番号蓄積手段に蓄積された失効番号と同じかより大きな識別番号を持つサーバ証明書を発行することを特徴としてもよい。

【０２１１】

また、証明書発行装置は、サーバ証明書を失効させるときに、サーバ証明書の識別番号を取得し、新たな失効番号として識別番号より大きな番号を失効番号として決定し、失効番号蓄積手段に蓄積し、サーバ証明書情報蓄積手段を検索し、サーバ証明書の識別番号と同じかより小さな識別番号を持つサーバ証明書（以下更新対象サーバ証明書）を取り出し、更新対象サーバ証明書を持つサーバに対して新たな失効番号と同じかより大きな識別番号を持つサーバ証明書に更新する構成としてもよい。

【０２１２】

また、証明書発行装置は、サーバ証明書情報蓄積手段から期限に近づいたサーバ証明書を検索し、サーバ証明書の識別番号を取得し、新たな失効番号として識別番号より大きな番号を失効番号として決定し失効番号蓄積手段に蓄積し、サーバ証明書情報蓄積手段を検索し、サーバ証明書の識別番号と同じかより小さな識別番号を持つサーバ証明書（以下更新対象サーバ証明書）を取り出し、更新対象サーバ証明書を持つサーバに対して新たな失効番号と同じかより大きな識別番号

を持つサーバ証明書に更新する構成としてもよい。

【０２１３】

【発明の効果】

以上の説明から明らかなように、本発明に係る通信装置によれば、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断したり、従来のようにリポジトリからサイズの大きなＣＲＬを取得して、たくさんのリストを記憶し、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検索したりする必要がなくなり、通信装置は、リポジトリから失効番号を１つだけ取得し、これを記憶している１つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

【０２１４】

また、本発明に係る通信装置によれば、通信装置は、サーバ装置との通信と同じ手順でリポジトリ証明書を取得し、リポジトリ証明書を用いてリポジトリを認証したり、リポジトリが正当である場合に失効番号を暗号通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

【０２１５】

また、本発明に係る通信装置によれば、通信装置は、リポジトリが正当である場合に失効番号を暗号なしの通信で取得したり、正常な失効番号だけを取得して、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。

【０２１６】

また、本発明に係る証明書発行装置によれば、従来のようにサーバ証明書の有効期限が過ぎたか否かを時計を用いて判断させたり、従来のようにリポジトリからサイズの大きなＣＲＬを取得させたりして、たくさんのリストを記憶させたりし、このたくさんのリストの中にサーバ証明書の識別番号が載っているか否か検

索させたりする必要がなくなり、通信装置は、リポジトリから失効番号を１つだけ取得し、これを記憶している１つの失効番号で、この失効番号が対象とする全てのサーバ証明書が有効か否かを判断することができる。したがって、通信装置及びリポジトリのメモリ容量などのリソースが簡単で済み、簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる。

【０２１７】

また、本発明に係る証明書発行装置によれば、有効期間が近づいたサーバー証明書を失効させることができる。

【０２１８】

また、本発明に係る証明書発行装置によれば、サーバ装置は、新たなサーバ証明書を用いて認証を受けることができる。

【０２１９】

よって、本発明により、極めて簡単なリソースでサーバ装置を認証することができ、インターネットが普及し、リソースが小さいネット家電装置等が登場しつつある今日における本願発明の実用的価値は極めて高い。

【図面の簡単な説明】

【図１】

本発明の実施の形態１に係る通信システム１の全体構成を示すブロック図である。

【図２】

図１に示されるサーバ証明書７５の構成例を示す図である。

【図３】

図１に示される失効情報９０の構成例を示す図である。

【図４】

図１に示されるサーバ証明書履歴テーブル１１０ａの構成例を示す図である。

【図５】

サーバ証明書組立部１０７が行う証明書用シリアル設定処理の動作を示すフローチャートである。

【図６】

サーバ証明書期限検索部１１１が行う証明書期限管理処理の動作を示すフローチャートである。

【図７】

失効証明書検索部１１３が有効期限到来による失効証明書検索処理の動作を示すフローチャートである。

【図８】

失効証明書検索部１１３が行う失効通知による失効証明書検索処理の動作を示すフローチャートである。

【図９】

失効情報署名部１１６が行う失効情報組立処理の動作を示すフローチャートである。

【図１０】

サーバ証明書検証部４３０の各部が行う失効情報取得処理の動作を示すフローチャートである。

【図１１】

暗号化して通信を行う場合のシーケンス図である。

【図１２】

サーバ証明書検証部４３０が行うサーバ証明書７５の検証動作を示すフローチャートである。

【図１３】

サーバが４台あったときのサーバ証明書７５のシリアルと失効番号との関係を示す図である。

【図１４】

本発明の実施の形態２に係る通信システム２の全体構成を示すブロック図である。

【図１５】

ＳＳＬ通信時における通信システムのシステム構成を示すブロック図である。

【図１６】

図１５に示されるサーバ証明書７０００の最小限の構成例を示す図である。

【図１７】

図１５に示されるＣＲＬ８０００の最小限の構成を示す図である。

【図１８】

暗号化せずに通信を行う場合のシーケンス図である。

【図１９】

暗号化して通信を行う場合のシーケンス図である。

【図２０】

サーバ証明書検証部４２００が行うサーバ証明書７０００の検証動作を示すフローチャートである。

【符号の説明】

１，２　通信システム

１０，１１　サーバ証明書作成装置

２０，２１　リポジトリ

３０ａ～３０ｋ　アプリケーションサーバ

４０ａ～４０ｎ，４１ａ～４１ｎ　端末

５０　インターネット５０

６０　ＣＡ証明書

７０　ＣＳＲ

７５　サーバ証明書

８０　失効通知

９０　失効情報

９０ｂ　失効情報

１０１　鍵ペア作成部

１０２　ＣＡ証明書作成部

１０３　ＣＡ秘密鍵蓄積部

１０４　時計

１０５　シリアル蓄積部

１０６　ＣＳＲ受信部

１０７　サーバ証明書組立部
１０８　署名部
１０９　サーバ証明書送信部
１１０　サーバ証明書履歴蓄積部
１１０ａ　サーバ証明書履歴テーブル
１１１　サーバ証明書期限検索部
１１２　サーバ証明書失効通知部
１１３　失効証明書検索部
１１４　証明書失効通知部
１１５　失効番号蓄積部
１１６　失効情報署名部
１１７　失効情報通知部
１２１　失効番号蓄積部
１２２　失効番号通知部
２０１　失効情報蓄積部
２０２　通信部
２０３　鍵ペア作成部
２０４　ＣＳＲ作成部
２０５　サーバ秘密鍵蓄積部
２０７　サーバ証明書蓄積部
２０８　失効情報蓄積部
２０９　通信部
３０１　鍵ペア作成部
３０２　ＣＳＲ作成部
３０３　サーバ秘密鍵蓄積部
３０４　サーバ証明書蓄積部
３０５　アプリサーバ部
３０６　通信部
４１０　アプリクライアント部

４２０　通信部

４３０　サーバ証明書検証部

４３１　失効情報要求部

４３２　署名検証部

４３３　ＣＡ証明書蓄積部

４３４　署名検証部

４３５　失効番号検証部

４３６　失効番号蓄積部

４３７　証明書シリアル抽出部

４３８　失効判定部

４４０　通信部

４５０　サーバ証明書検証部

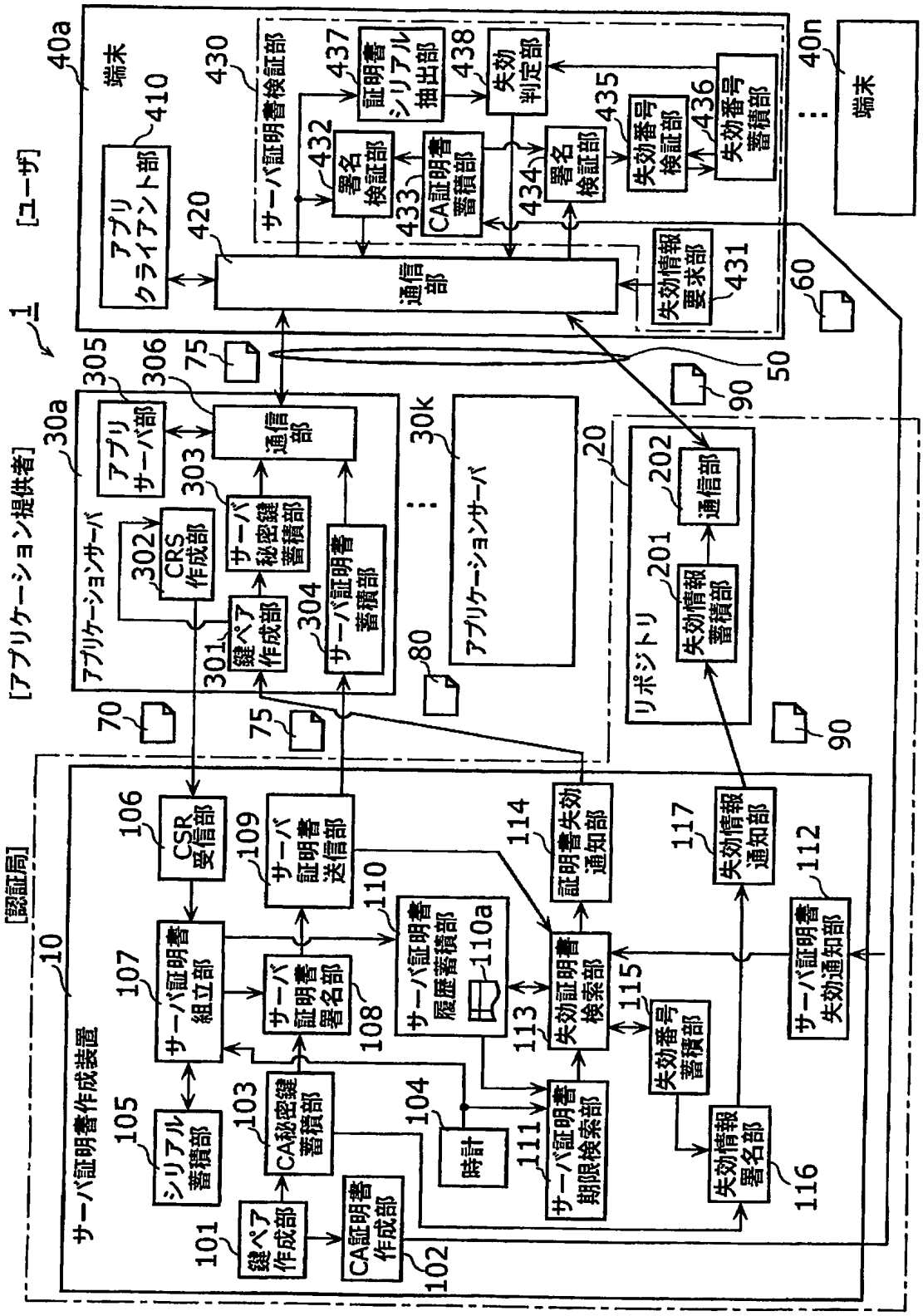
４５１　失効情報要求部

４５２　証明書シリアル抽出部

４５３　失効番号検証部

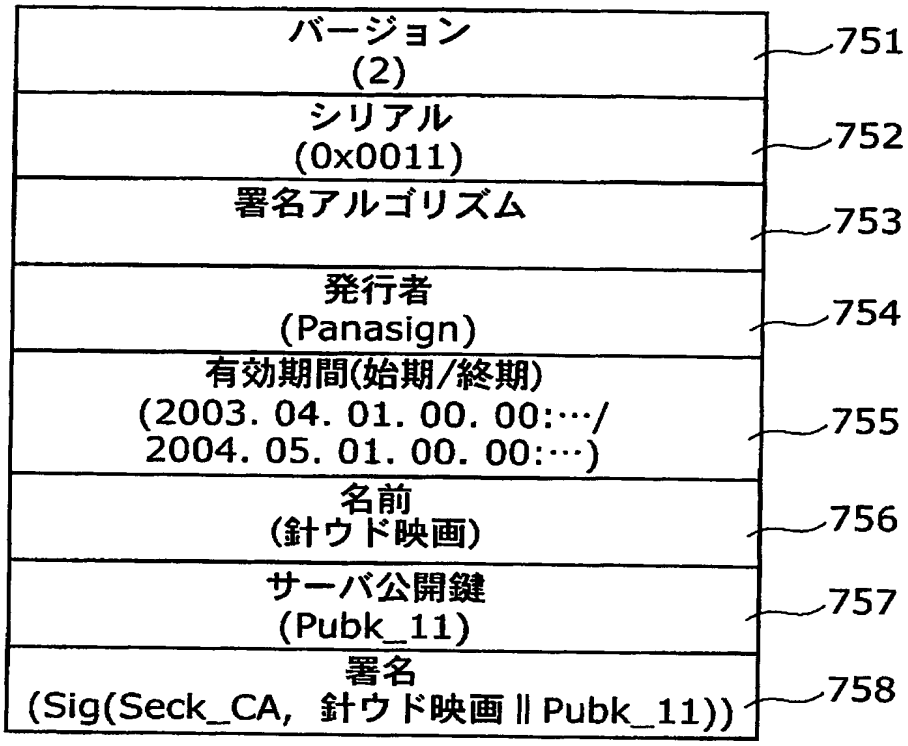
【書類名】　図面

【図１】


[認証局]
サーバ証明書作成装置
10
CSR受信部
106
サーバ証明書組立部
107
サーバ証明書署名部
108
サーバ証明書送信部
109
サーバ証明書履歴蓄積部
110
110a
証明書失効通知部
114
失効情報通知部
117
サーバ証明書失効通知部
112
シリアル蓄積部
105
CA秘密鍵蓄積部
103
時計
104
サーバ証明書期限検索部
111
失効証明書検索部
113
失効番号蓄積部
115
失効情報署名部
116
鍵ペア作成部
101
CA証明書作成部
102
[アプリケーション提供者]
アプリケーションサーバ
30a
アプリサーバ部
305
通信部
306
CRS作成部
302
サーバ秘密鍵蓄積部
303
鍵ペア作成部
301
サーバ証明書蓄積部
304
アプリケーションサーバ
30k
リポジトリ
20
通信部
202
失効情報蓄積部
201
70
75
80
90
50
60
[ユーザ]
1
端末
40a
アプリクライアント部
410
通信部
420
サーバ証明書検証部
430
署名検証部
432
CA証明書蓄積部
433
証明書シリアル抽出部
437
失効判定部
438
署名検証部
434
失効番号検証部
435
失効番号蓄積部
436
失効情報要求部
431
端末
40n

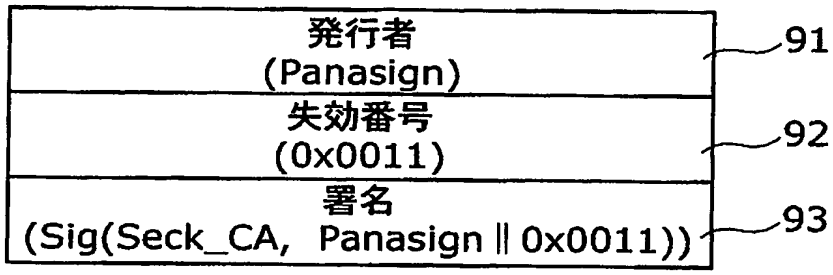
【図２】

サーバ証明書75

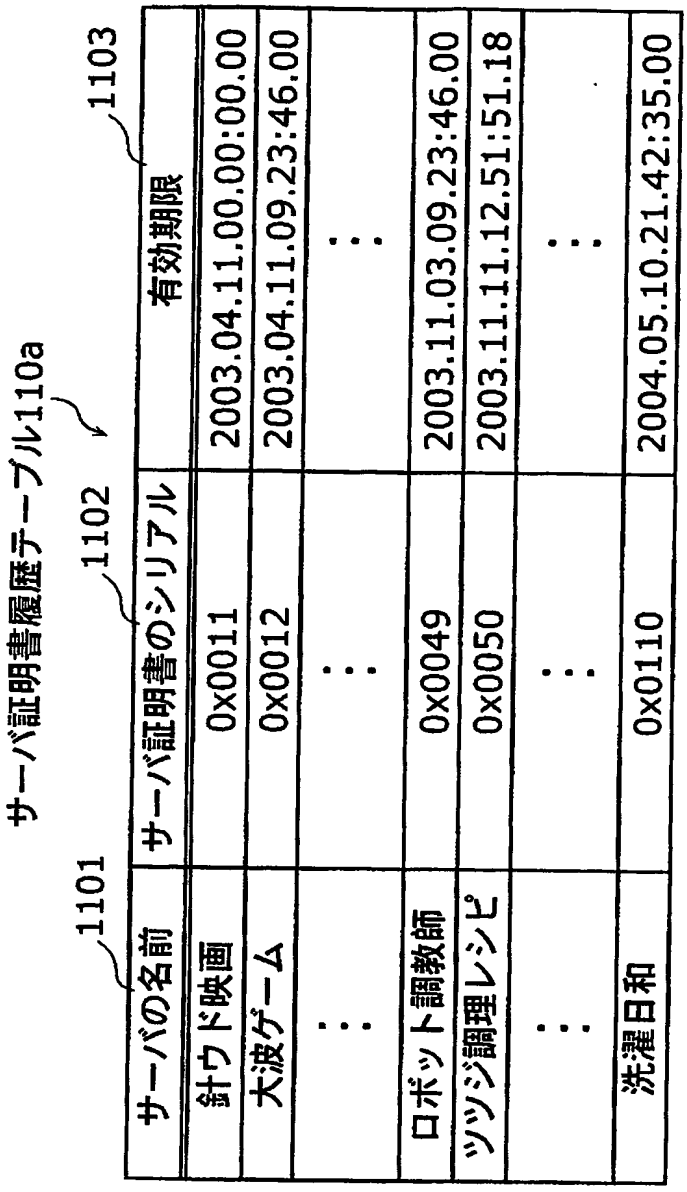


【図３】

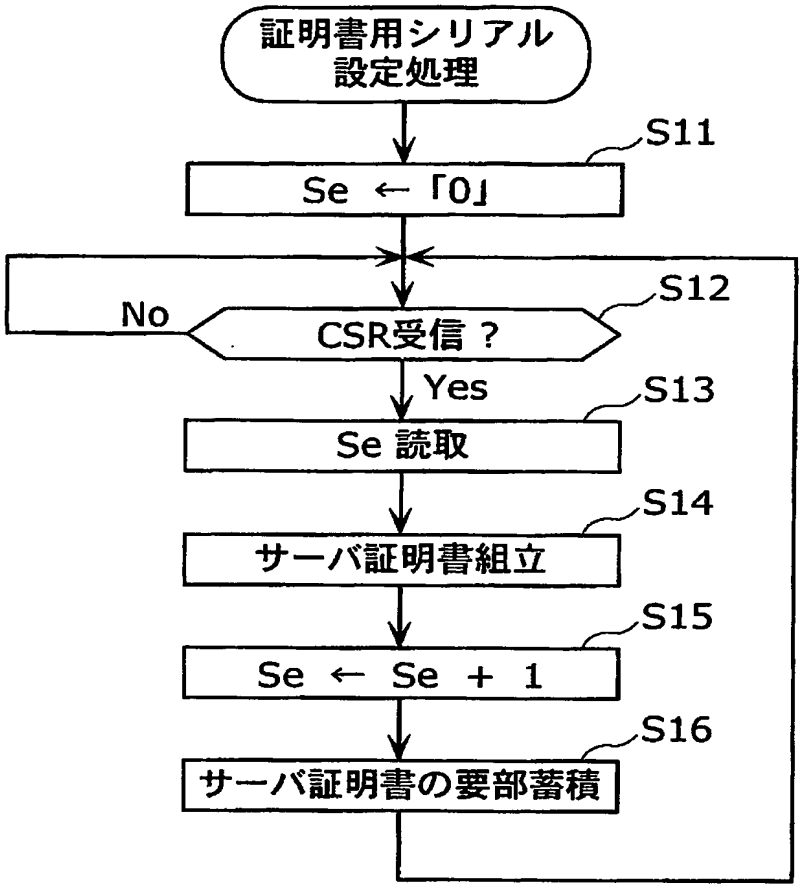
失効情報 90



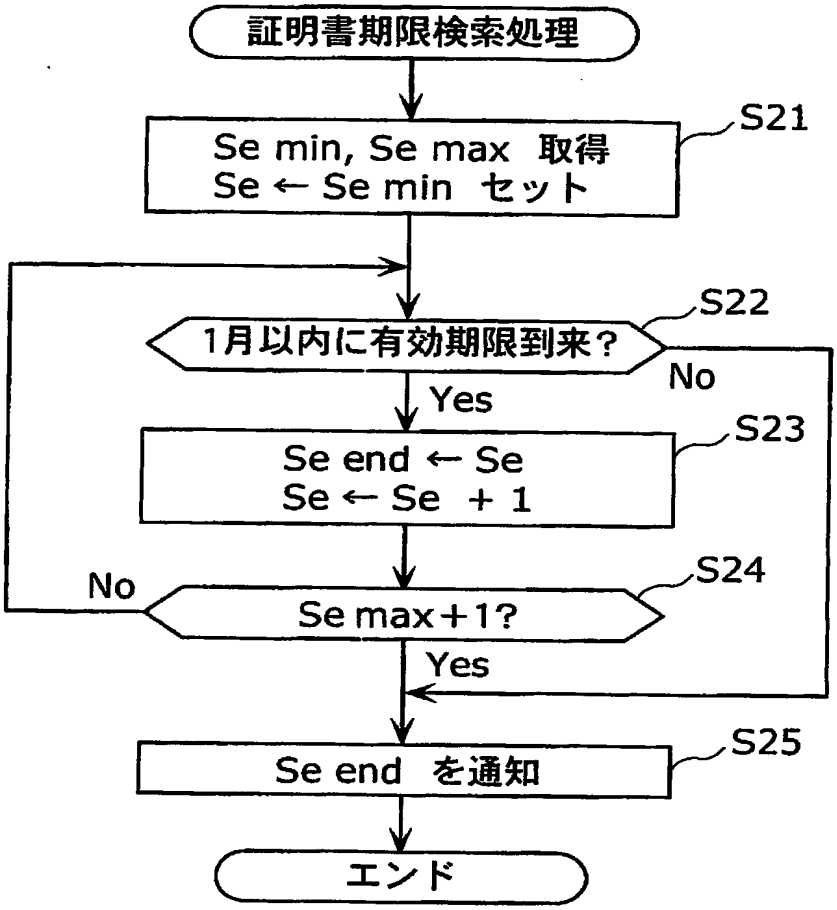
【図４】


サーバ証明書履歴テーブル110a
1101
1102
1103
サーバの名前
サーバ証明書のシリアル
有効期限
針ウド映画
0x0011
2003.04.11.00.00:00.00
大波ゲーム
0x0012
2003.04.11.09.23:46.00
ロボット調教師
0x0049
2003.11.03.09.23:46.00
ツツジ調理レシピ
0x0050
2003.11.11.12.51:51.18
洗濯日和
0x0110
2004.05.10.21.42:35.00

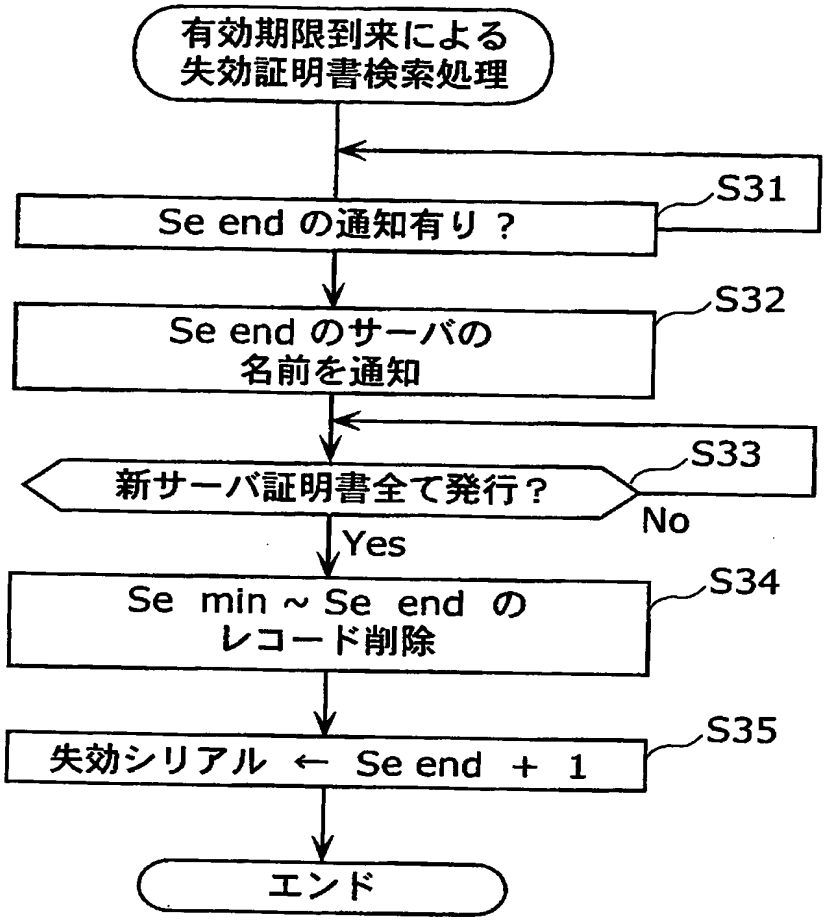
【図５】


証明書用シリアル
設定処理
S11
Se ← 「0」
S12
No
CSR受信？
Yes
S13
Se 読取
S14
サーバ証明書組立
S15
Se ← Se + 1
S16
サーバ証明書の要部蓄積

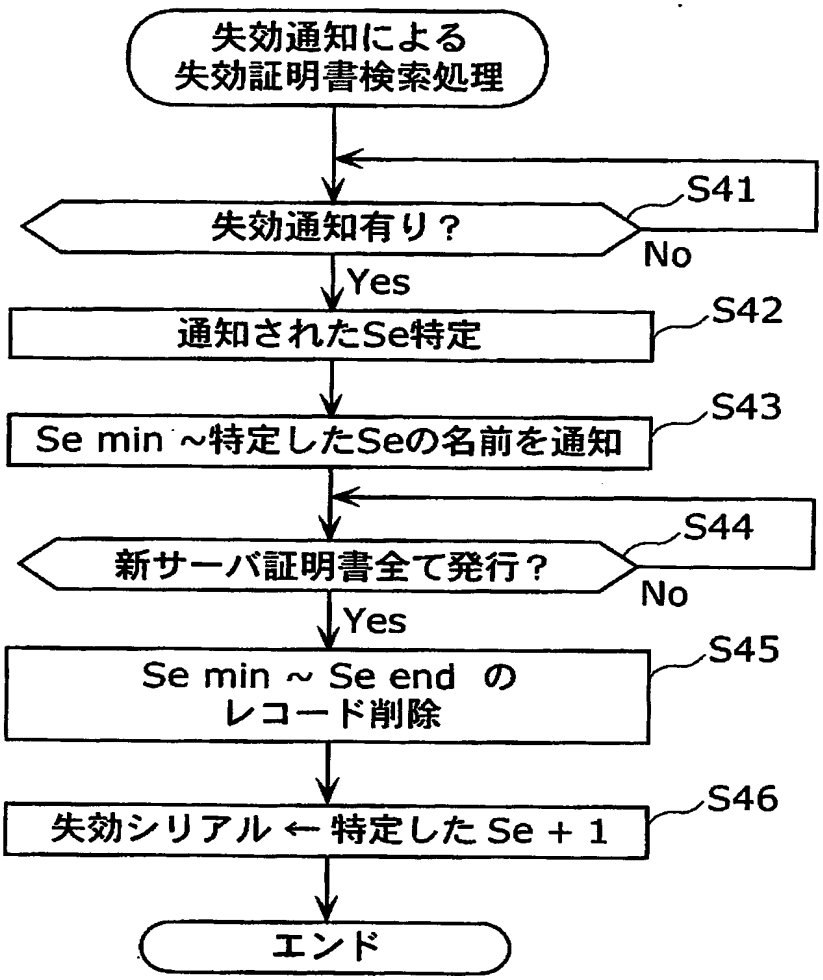
【図６】


証明書期限検索処理
Se min, Se max 取得
Se ← Se min セット
S21
1月以内に有効期限到来？
S22
No
Yes
Se end ← Se
Se ← Se + 1
S23
No
Se max+1?
S24
Yes
Se end を通知
S25
エンド

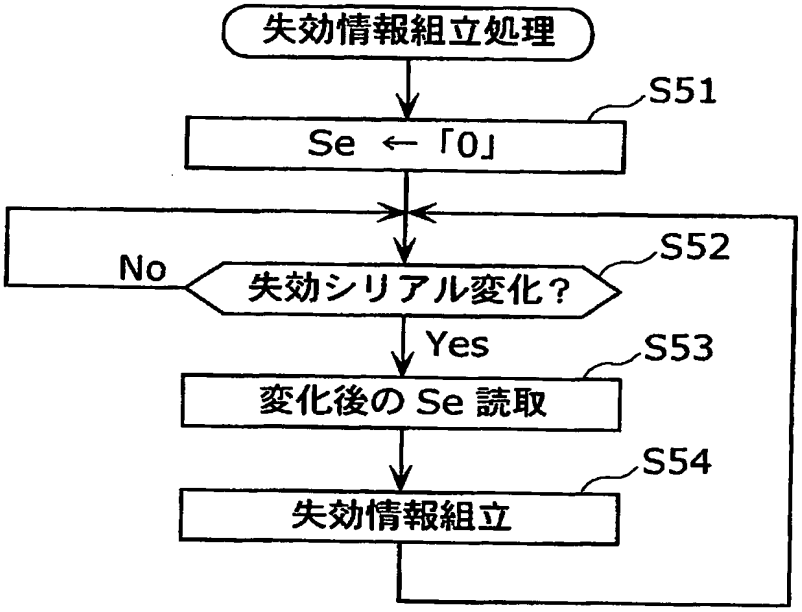
【図７】


有効期限到来による
失効証明書検索処理
S31
Se end の通知有り？
S32
Se end のサーバの
名前を通知
S33
新サーバ証明書全て発行？
No
Yes
S34
Se min ~ Se end の
レコード削除
S35
失効シリアル ← Se end + 1
エンド

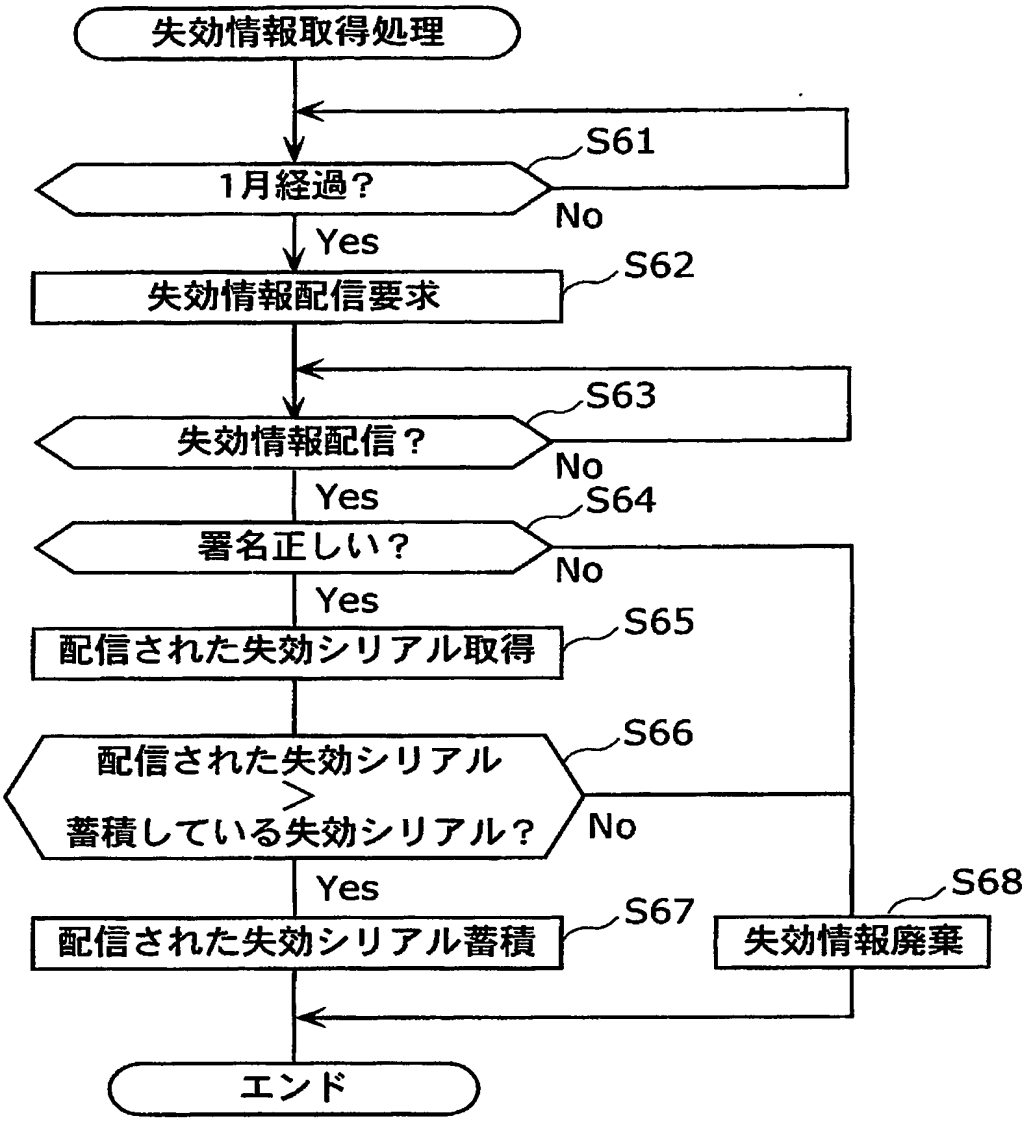
【図８】


失効通知による
失効証明書検索処理
S41
失効通知有り？
No
Yes
S42
通知されたSe特定
S43
Se min ~特定したSeの名前を通知
S44
新サーバ証明書全て発行？
No
Yes
S45
Se min ~ Se end の
レコード削除
S46
失効シリアル ← 特定した Se + 1
エンド

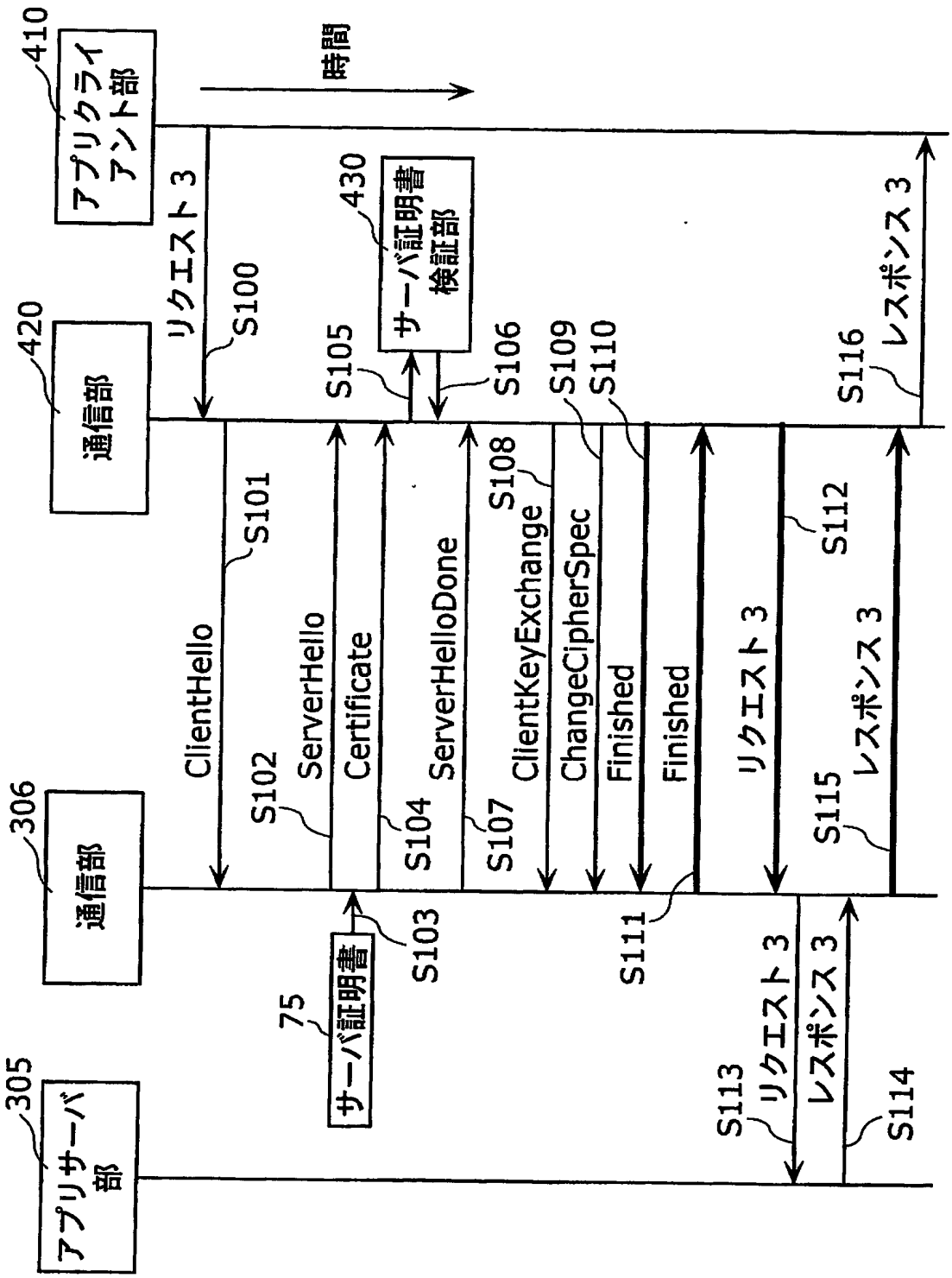
【図９】


失効情報組立処理
S51
Se ← 「0」
S52
No
失効シリアル変化？
Yes
S53
変化後の Se 読取
S54
失効情報組立

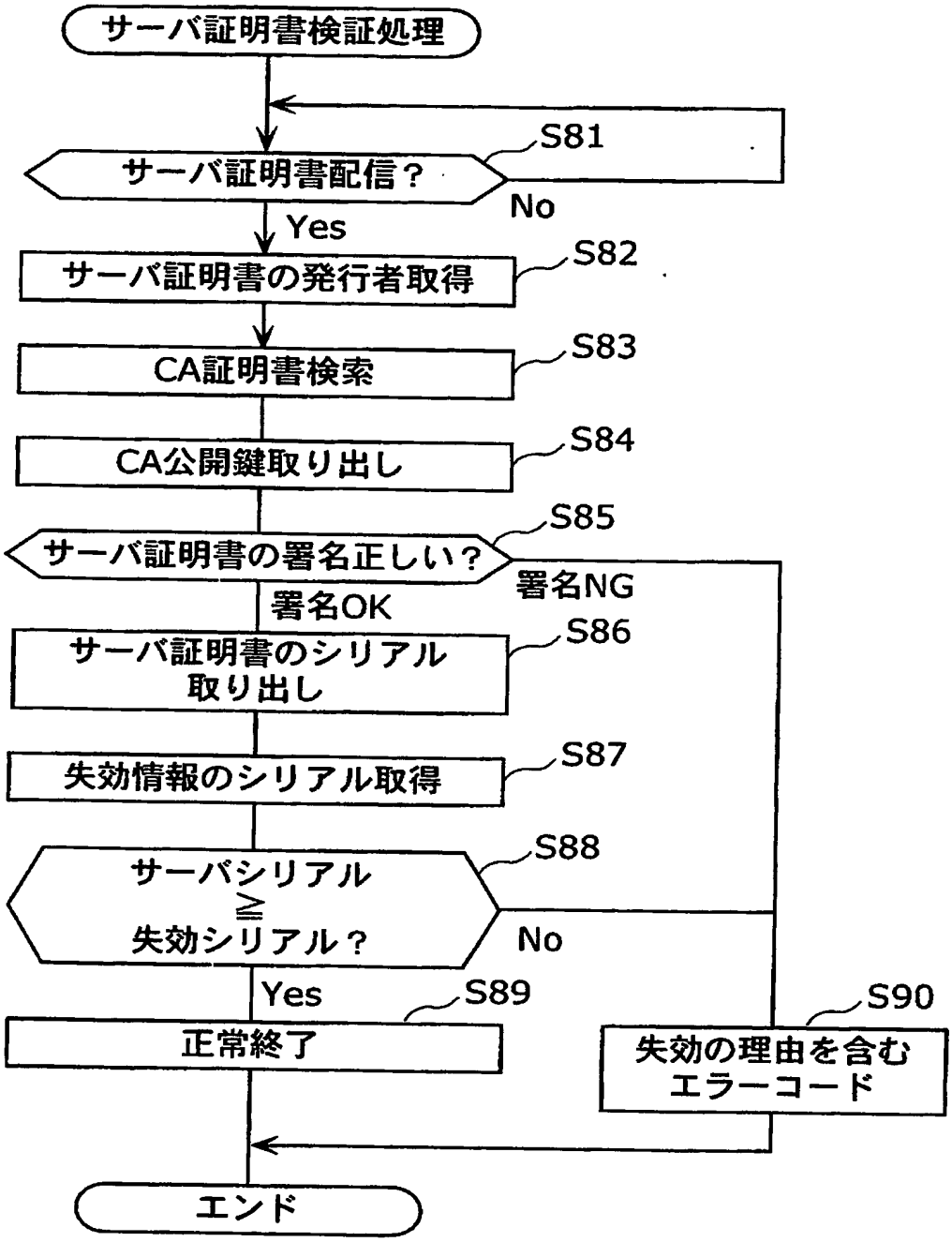
【図１０】


失効情報取得処理
S61
1月経過？
No
Yes
S62
失効情報配信要求
S63
失効情報配信？
No
Yes
S64
署名正しい？
No
Yes
S65
配信された失効シリアル取得
S66
配信された失効シリアル
＞
蓄積している失効シリアル？
No
Yes
S67
配信された失効シリアル蓄積
S68
失効情報廃棄
エンド

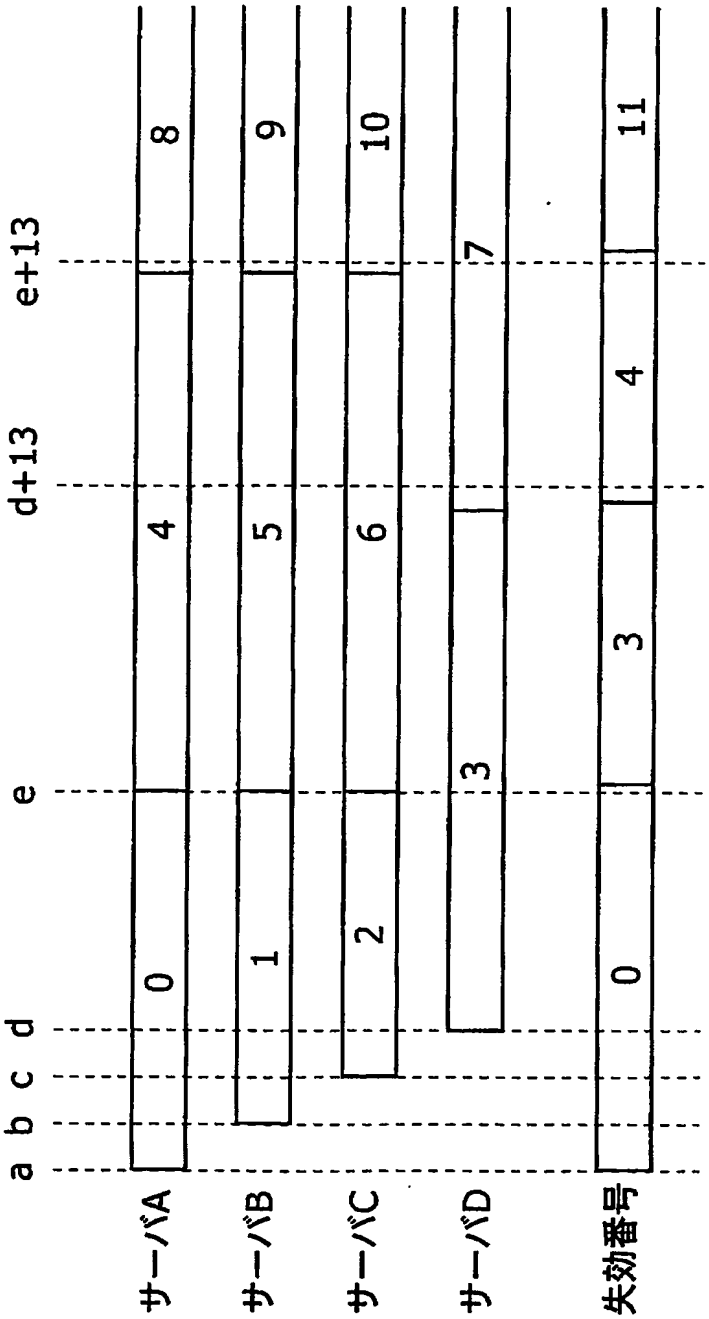
【図１１】


410
アプリクライアント部
時間
420
通信部
リクエスト３
S100
430
サーバ証明書検証部
S105
S106
S109
S110
S116
レスポンス３
S101
ClientHello
S102
ServerHello
Certificate
S104
ServerHelloDone
S107
S108
ClientKeyExchange
ChangeCipherSpec
Finished
Finished
S111
リクエスト３
S112
S115
レスポンス３
306
通信部
75
サーバ証明書
S103
305
アプリサーバ部
S113
リクエスト３
レスポンス３
S114

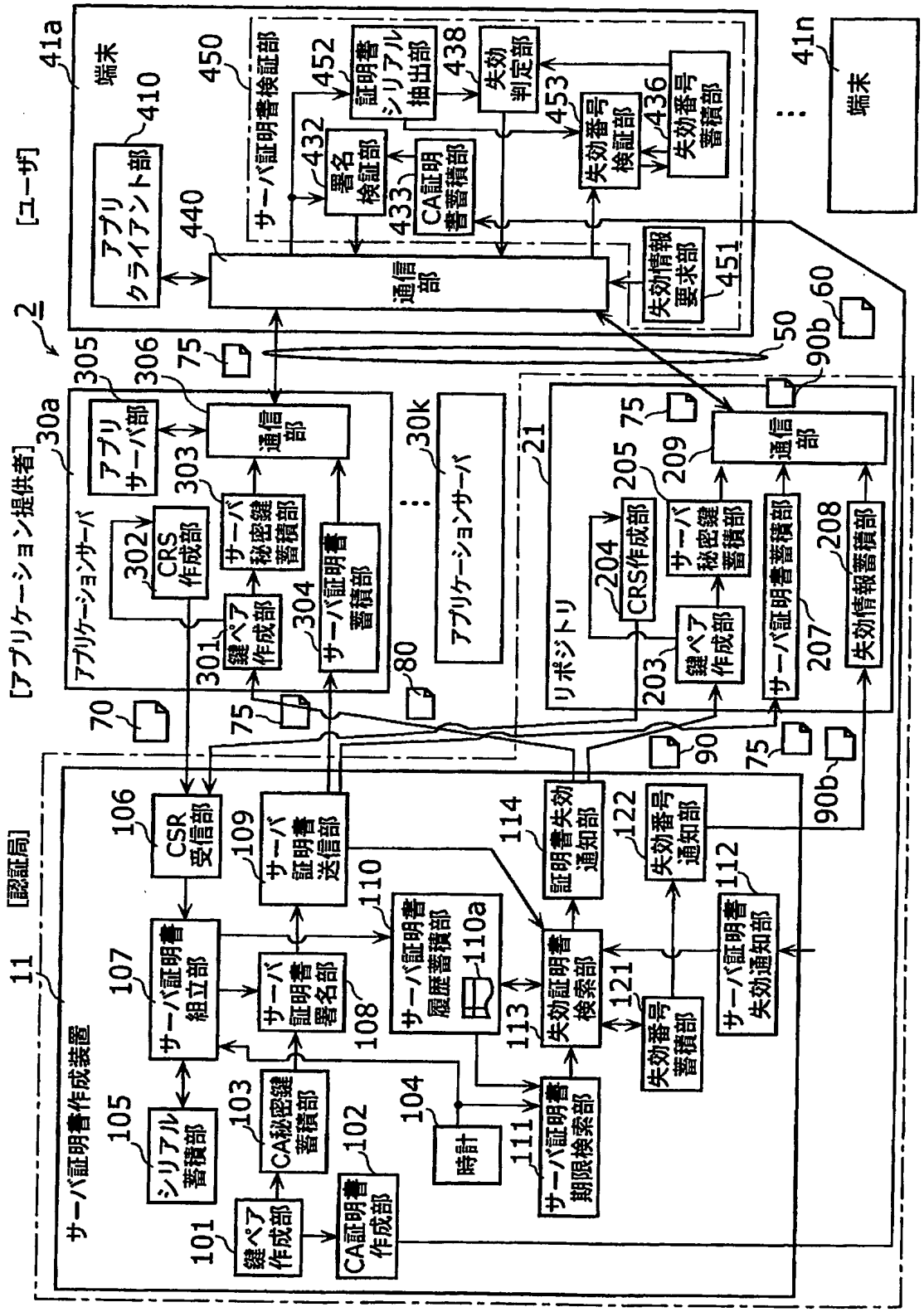
【図１２】


サーバ証明書検証処理
S81
サーバ証明書配信？
No
Yes
S82
サーバ証明書の発行者取得
S83
CA証明書検索
S84
CA公開鍵取り出し
S85
サーバ証明書の署名正しい？
署名NG
署名OK
S86
サーバ証明書のシリアル
取り出し
S87
失効情報のシリアル取得
S88
サーバシリアル
≧
失効シリアル？
No
Yes
S89
正常終了
S90
失効の理由を含む
エラーコード
エンド

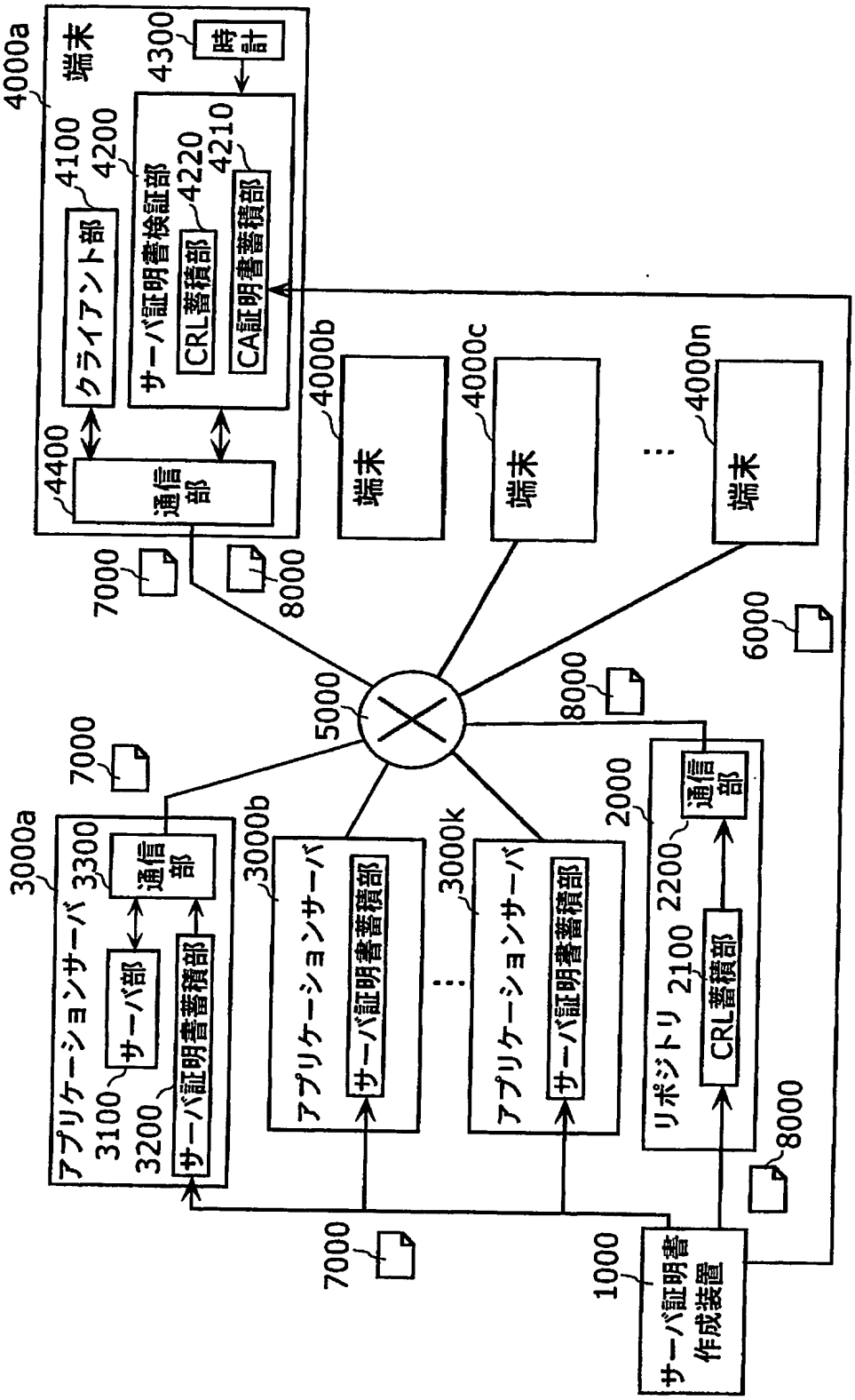
【図１３】



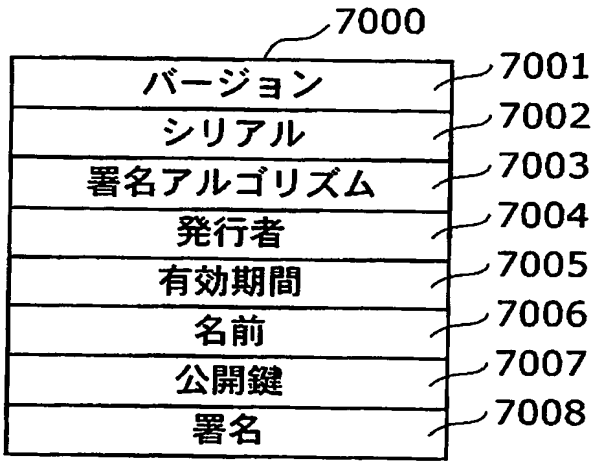
【図１４】


[認証局]
11
サーバ証明書作成装置
101 鍵ペア作成部
102 CA証明書作成部
103 CA秘密鍵蓄積部
104 時計
105 シリアル蓄積部
106 CSR受信部
107 サーバ証明書組立部
108 サーバ証明書署名部
109 サーバ証明書送信部
110 サーバ証明書履歴蓄積部
110a
111 サーバ証明書期限検索部
112 サーバ証明書失効通知部
113 失効証明書検索部
114 証明書失効通知部
121 失効番号蓄積部
122 失効番号通知部
[アプリケーション提供者]
30a アプリケーションサーバ
30k アプリケーションサーバ
301 鍵ペア作成部
302 CRS作成部
303 サーバ秘密鍵蓄積部
304 サーバ証明書蓄積部
305 アプリサーバ部
306 通信部
2
[ユーザ]
41a 端末
41n 端末
410 アプリクライアント部
440 通信部
450 サーバ証明書検証部
451 失効情報要求部
452 証明書シリアル抽出部
453 失効判定部
432 署名検証部
433 CA証明書蓄積部
436 失効番号蓄積部
438
21 リポジトリ
203 鍵ペア作成部
204 CRS作成部
205 サーバ秘密鍵蓄積部
207 サーバ証明書蓄積部
208 失効情報蓄積部
209 通信部
50
60
70
75
80
90
90b

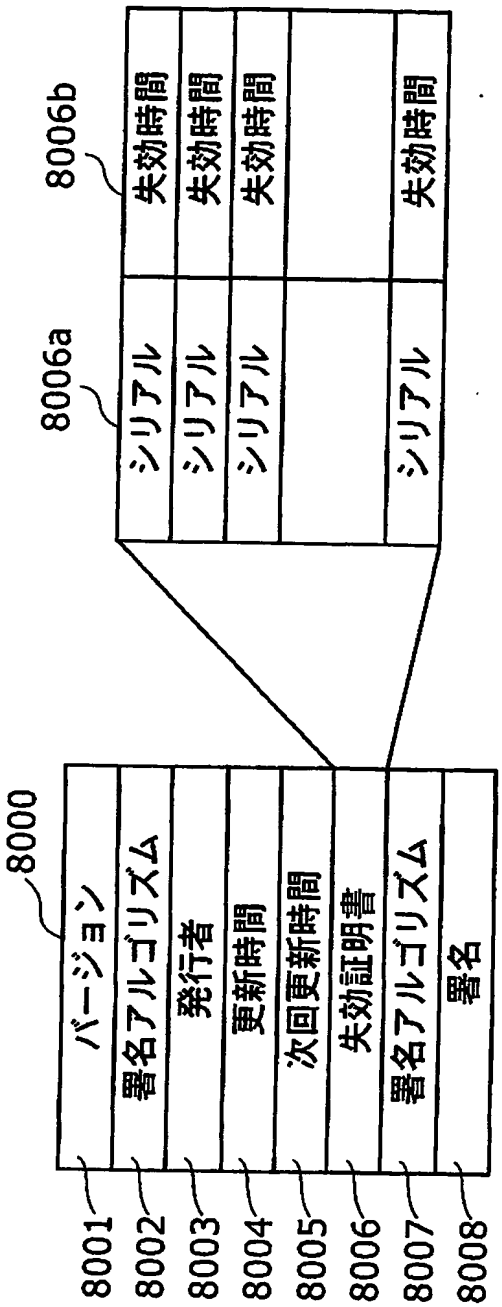
【図１５】


4000a
端末
4300
時計
4100
クライアント部
4200
サーバ証明書検証部
4220
CRL蓄積部
4210
CA証明書蓄積部
4400
通信部
4000b
端末
4000c
端末
4000n
端末
7000
8000
6000
5000
3000a
アプリケーションサーバ
3300
通信部
3100
サーバ部
3200
サーバ証明書蓄積部
3000b
アプリケーションサーバ
サーバ証明書蓄積部
3000k
アプリケーションサーバ
サーバ証明書蓄積部
2000
通信部
2200
リポジトリ
2100
CRL蓄積部
1000
サーバ証明書作成装置

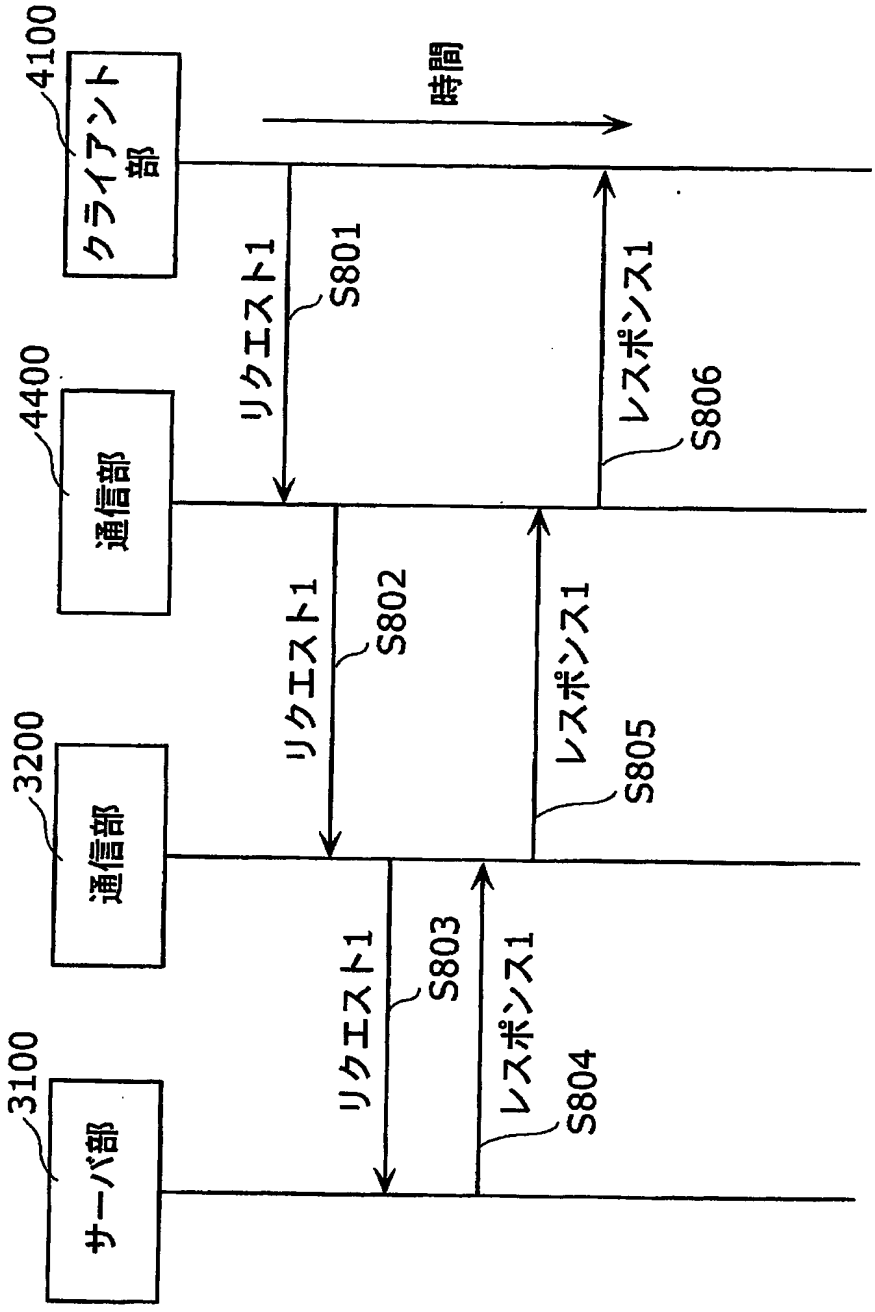
【図１６】


7000
バージョン
7001
シリアル
7002
署名アルゴリズム
7003
発行者
7004
有効期間
7005
名前
7006
公開鍵
7007
署名
7008

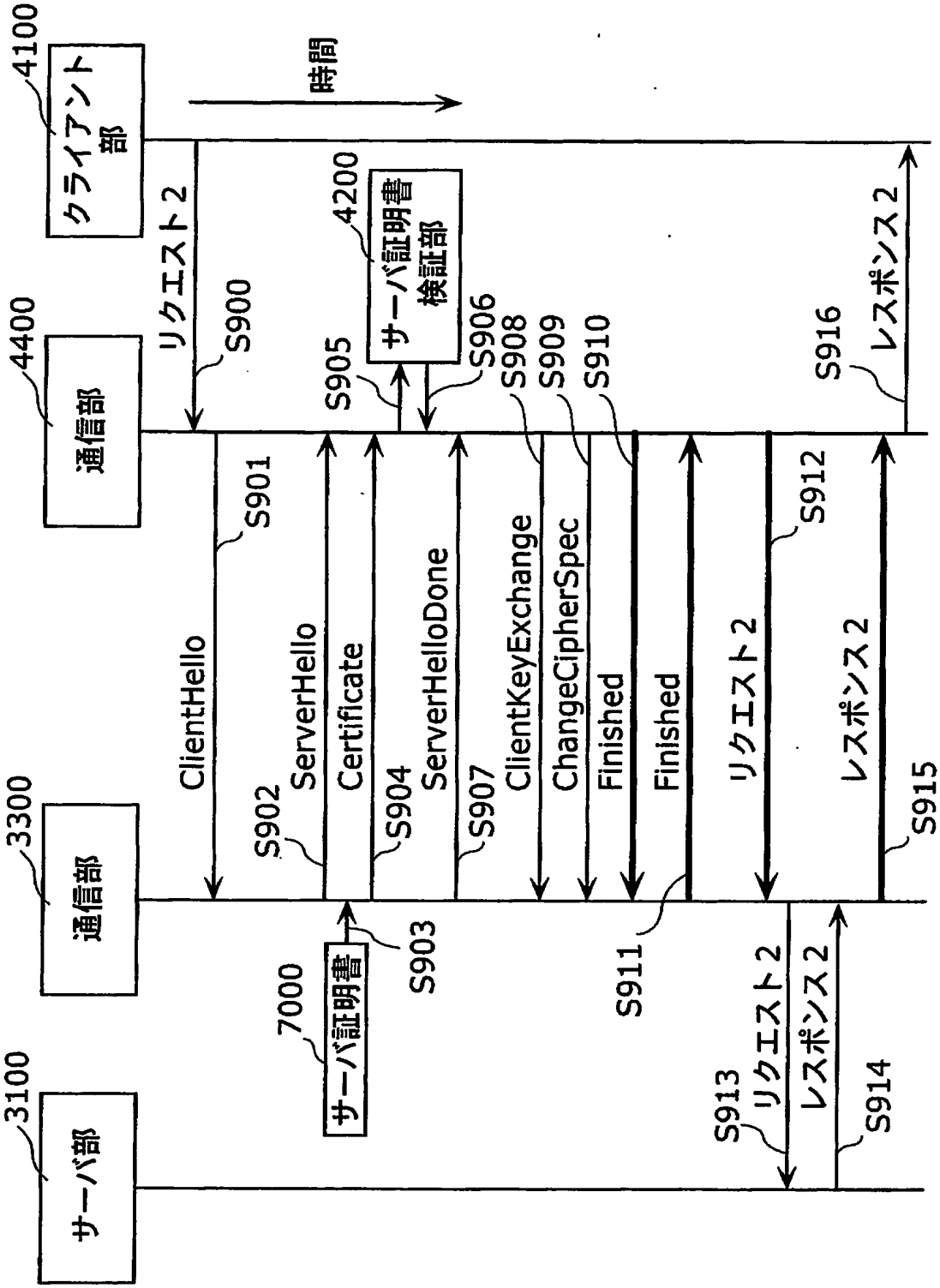
【図１７】


8000
バージョン
署名アルゴリズム
発行者
更新時間
次回更新時間
失効証明書
署名アルゴリズム
署名
8001
8002
8003
8004
8005
8006
8007
8008
8006a
シリアル
シリアル
シリアル
シリアル
8006b
失効時間
失効時間
失効時間
失効時間

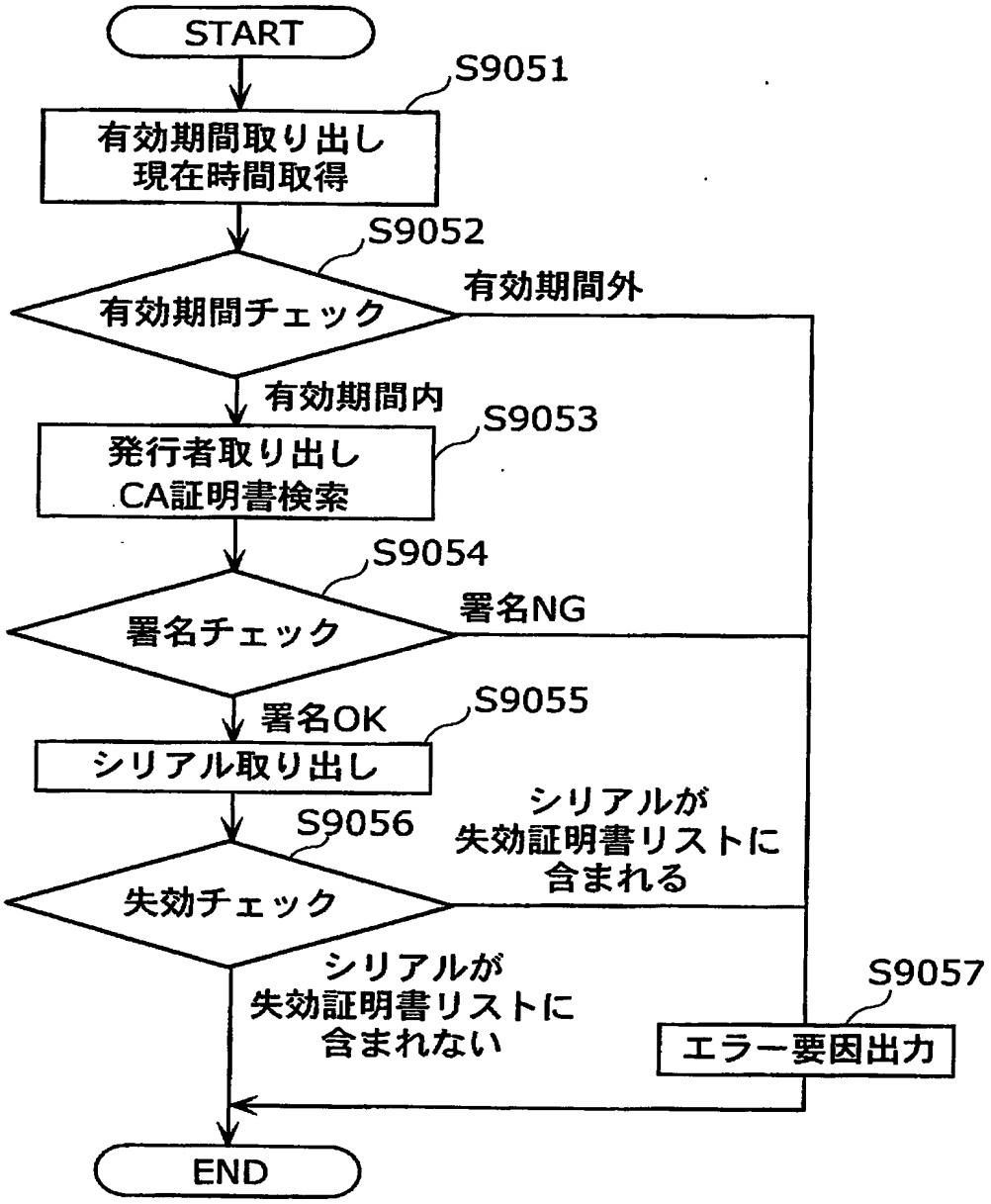
【図１８】


4100
クライアント部
時間
リクエスト1
S801
レスポンス1
S806
4400
通信部
リクエスト1
S802
レスポンス1
S805
3200
通信部
リクエスト1
S803
レスポンス1
S804
3100
サーバ部

【図１９】


4100
クライアント部
時間
4200
サーバ証明書検証部
4400
通信部
リクエスト2
S900
S905
S906
S908
S909
S910
S916
レスポンス2
S901
S912
3300
通信部
ClientHello
S902
ServerHello
Certificate
S904
ServerHelloDone
S907
ClientKeyExchange
ChangeCipherSpec
Finished
Finished
リクエスト2
レスポンス2
S915
7000
サーバ証明書
S903
S911
3100
サーバ部
S913
リクエスト2
レスポンス2
S914

【図２０】


START
S9051
有効期間取り出し
現在時間取得
S9052
有効期間チェック
有効期間外
有効期間内
S9053
発行者取り出し
CA証明書検索
S9054
署名チェック
署名NG
署名OK
S9055
シリアル取り出し
S9056
シリアルが
失効証明書リストに
含まれる
失効チェック
シリアルが
失効証明書リストに
含まれない
S9057
エラー要因出力
END

【書類名】　　要約書

【要約】

【課題】　簡単なリソースでサーバ装置の正当性を示すサーバ証明書に基づいて当該サーバ装置と通信することができる通信装置を提供する。

【解決手段】　端末４０ａは、サーバ証明書７５の有効性を判断する基準となる情報である失効番号を保持するリポジトリ２０から、失効番号を取得する失効番号検証部４３５と、取得された失効番号を記憶する失効番号蓄積部４３６と、サーバ証明書７５を識別する識別番号をサーバ証明書７５から読み出す証明書シリアル抽出部４３７と、読み出された識別番号と失効番号蓄積部４３６に記憶されている失効番号とを比較することによってサーバ証明書７５の有効性を判断する失効判定部４３８と、サーバ証明書７５が有効であると判断された場合に、アプリケーションサーバ３０ａとの通信を確立し、サーバ証明書７５が有効でないと判断された場合に、アプリケーションサーバ３０ａとの通信を確立しない通信部４２０とを備える。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－１００８６６
受付番号	５０３００５６０４７０
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　４月　４日

＜認定情報・付加情報＞

【提出日】　平成15年 4月 3日

次頁無

特願２００３－１００８６６

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社